

14.10.99

日本国特許庁

PATENT OFFICE
JAPANESE GOVERNMENT

REC'D 29 OCT 1999

WIPO PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日

Date of Application:

1998年10月19日

出願番号

Application Number:

平成10年特許願第296942号

出願人

Applicant (s):

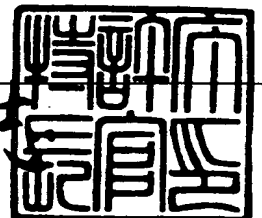
ソニー株式会社

PRIORITY
DOCUMENTSUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a)OR(b)

1999年 8月24日

特許庁長官
Commissioner,
Patent Office

伴佐山 建志



出証番号 出証特平11-3059144

【書類名】 特許願

【整理番号】 9801034108

【提出日】 平成10年10月19日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/16

【発明の名称】 情報処理装置および方法、管理装置および方法、情報利用システム、提供媒体、並びに外部記憶媒体

【請求項の数】 9

【発明者】

 【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
 内

 【氏名】 石橋 義人

【発明者】

 【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
 内

 【氏名】 北原 淳

【特許出願人】

 【識別番号】 000002185

 【氏名又は名称】 ソニー株式会社

 【代表者】 出井 伸之

【代理人】

 【識別番号】 100082131

 【弁理士】

 【氏名又は名称】 稲本 義雄

 【電話番号】 03-3369-6479

【手数料の表示】

 【予納台帳番号】 032089

 【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9708842

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理装置および方法、管理装置および方法、情報利用システム、提供媒体、並びに外部記憶媒体

【特許請求の範囲】

【請求項1】 装着された外部記憶媒体に所定の情報を記憶させると共に、暗号化された情報を復号し、利用する情報処理装置において、装着された前記外部記憶媒体と相互認証する相互認証手段と、所定の鍵で所定の情報を暗号化する暗号化手段とを備えることを特徴とする情報処理装置。

【請求項2】 前記所定の鍵は、前記情報処理装置を管理する管理装置の公開鍵である

ことを特徴とする請求項1に記載の情報処理装置。

【請求項3】 装着された外部記憶媒体に所定の情報を記憶させると共に、暗号化された情報を復号し、利用する情報処理装置の情報処理方法において、装着された前記外部記憶媒体と相互認証する相互認証ステップと、所定の鍵で所定の情報を暗号化する暗号化ステップとを含むことを特徴とする情報処理方法。

【請求項4】 装着された外部記憶媒体に所定の情報を記憶させると共に、暗号化された情報を復号し、利用する情報処理装置に、装着された前記外部記憶媒体と相互認証する相互認証ステップと、所定の鍵で所定の情報を暗号化する暗号化ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【請求項5】 暗号化された情報を復号し、利用する情報処理装置を管理する管理装置において、

前記情報処理装置に装着された外部記憶媒体に記憶されたデータを復号する復号手段

を備えることを特徴とする管理装置。

【請求項 6】 暗号化された情報を復号し、利用する情報処理装置を管理する管理方法において、

前記情報処理装置に装着された外部記憶媒体に記憶されたデータを復号する復号ステップ

を含むことを特徴とする管理方法。

【請求項 7】 暗号化された情報を復号し、利用する情報処理装置を管理する管理装置に、

前記情報処理装置に装着された外部記憶媒体に記憶されたデータを復号する復号ステップ

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【請求項 8】 装着された外部記憶媒体に所定の情報を記憶させると共に、暗号化された情報を復号し、利用する情報処理装置、および前記情報処理装置を管理する管理装置からなる情報利用システムにおいて、

前記情報処理装置は、

装着された前記外部記憶媒体と相互認証する相互認証手段と、

前記管理装置の公開鍵で所定の情報を暗号化する暗号化手段と、

を備え、

前記管理装置は、

前記外部記憶媒体に記憶されたデータを復号する復号手段

を備えることを特徴とする情報利用システム。

【請求項 9】 暗号化された情報を復号し、利用する情報処理装置に装着される外部記憶媒体において、

前記情報処理装置と相互認証する相互認証手段

を備えることを特徴とする外部記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報処理装置および方法、管理装置および方法、情報利用システム

、提供媒体、並びに外部記憶媒体に関し、特に、暗号化された情報を利用する情報処理装置および方法、管理装置および方法、情報利用システム、提供媒体、並びに外部記憶媒体に関する。

【0002】

【従来の技術】

音楽などの情報を暗号化し、所定の契約を交わしたユーザの情報処理装置に送信し、ユーザは、その情報処理装置で情報を復号して、再生するシステムがある。この情報処理装置において、情報の復号に必要な鍵および課金情報など所定の情報は、外部からの不正アクセスを排除できる記憶部に記憶される。

【0003】

【発明が解決しようとする課題】

しかし、新たな機器を利用する場合、情報の提供者と再度、契約を行う必要がある。また、何らかの原因で、外部からの不正アクセスを排除できる記憶部に記憶された情報が破壊された場合、ユーザには、契約しているにもかかわらず、情報が利用できず、情報提供者には、利用済みの情報に対する課金情報等が利用できなければ、決済が不可能になる等の問題が発生する。また、外部からの不正アクセスを排除できる記憶部に記憶される情報をそのまま外部に記憶したのでは、不正に対する安全性が低下する。

【0004】

本発明はこのような状況に鑑みてなされたものであり、不正に対する安全性を保持したまま、必要な情報を外部に記憶できるようにすることを目的とする。

【0005】

【課題を解決するための手段】

請求項1に記載の情報処理装置は、装着された外部記憶媒体と相互認証する相互認証手段と、所定の鍵で所定の情報を暗号化する暗号化手段とを備えることを特徴とする。

【0006】

請求項3に記載の情報処理方法は、装着された外部記憶媒体と相互認証する相互認証ステップと、所定の鍵で所定の情報を暗号化する暗号化ステップとを含む

ことを特徴とする。

【0007】

請求項4に記載の提供媒体は、情報処理装置に、装着された外部記憶媒体と相互認証する相互認証ステップと、所定の鍵で所定の情報を暗号化する暗号化ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【0008】

請求項5に記載の管理装置は、情報処理装置に装着された外部記憶媒体に記憶されたデータを復号する復号手段を備えることを特徴とする。

【0009】

請求項6に記載の管理方法は、情報処理装置に装着された外部記憶媒体に記憶されたデータを復号する復号ステップを含むことを特徴とする。

【0010】

請求項7に記載の提供媒体は、管理装置に、情報処理装置に装着された外部記憶媒体に記憶されたデータを復号する復号ステップを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【0011】

請求項8に記載の情報利用システムは、情報処理装置が、装着された外部記憶媒体と相互認証する相互認証手段と、管理装置の公開鍵で所定の情報を暗号化する暗号化手段とを備え、管理装置が、外部記憶媒体に記憶されたデータを復号する復号手段を備えることを特徴とする。

【0012】

請求項9に記載の外部記憶媒体は、情報処理装置と相互認証する相互認証手段を備えることを特徴とする。

【0013】

請求項1に記載の情報処理装置、請求項3に記載の情報処理方法、および請求項4に記載の提供媒体においては、装着された外部記憶媒体と相互認証し、所定の鍵で所定の情報を暗号化する。

【0014】

請求項5に記載の管理装置、請求項6に記載の管理方法、および請求項7に記載の提供媒体においては、情報処理装置に装着された外部記憶媒体に記憶されたデータを復号する。

【0015】

請求項8に記載の情報利用システムにおいては、情報処理装置が、装着された外部記憶媒体と相互認証し、管理装置の公開鍵で所定の情報を暗号化し、管理装置が、外部記憶媒体に記憶されたデータを復号する。

【0016】

請求項9に記載の外部記憶媒体においては、情報処理装置と相互認証する。

【0017】

【発明の実施の形態】

以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付加して本発明の特徴を記述すると、次のようになる。但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

【0018】

すなわち、請求項1に記載の情報処理装置は、装着された外部記憶媒体と相互認証する相互認証手段（例えば、図10の相互認証モジュール71）と、所定の鍵で所定の情報を暗号化する暗号化手段（例えば、図10の暗号化ユニット93）とを備えることを特徴とする。

【0019】

請求項5に記載の管理装置は、情報処理装置に装着された外部記憶媒体に記憶されたデータを復号する復号手段（例えば、図2のユーザ管理部18）を備えることを特徴とする。

【0020】

請求項8に記載の情報利用システムは、情報処理装置が、装着された外部記憶媒体と相互認証する相互認証手段（例えば、図10の相互認証モジュール71）

と、管理装置の公開鍵で所定の情報を暗号化する暗号化手段（例えば、図10の暗号化ユニット93）とを備え、管理装置が、外部記憶媒体に記憶されたデータを復号する復号手段（例えば、図2のユーザ管理部18）を備えることを特徴とする。

【0021】

請求項9に記載の外部記憶媒体は、情報処理装置と相互認証する相互認証手段（例えば、図10の相互認証モジュール81）を備えることを特徴とする。

【0022】

図1は、本発明を適用したEMD(Electronic Music Distribution:電子音楽配信)システムを説明する図である。このシステムでユーザに配信されるコンテンツ(Content)とは、情報そのものが価値を有するデジタルデータをいい、以下、音楽データを例に説明する。EMDサービスセンタ1は、コンテンツプロバイダ2、ユーザホームネットワーク5等に配送用鍵Kdを送信し、ユーザホームネットワーク5から、コンテンツの利用に応じた課金情報等を受信し、利用料金を精算し、コンテンツプロバイダ2およびサービスプロバイダ3への利益分配の処理を行う。

【0023】

コンテンツプロバイダ2は、デジタル化されたコンテンツを有し、自己のコンテンツであることを証明するためのウォーターマーク（電子透かし）をコンテンツに挿入し、コンテンツを圧縮し、および暗号化し、所定の情報を付加して、サービスプロバイダ3に送信する。

【0024】

サービスプロバイダ3は、専用のケーブルネットワーク、インターネット、または衛星などから構成されるネットワーク4を介して、コンテンツプロバイダ2から供給されたコンテンツに価格を付して、ユーザホームネットワーク5に送信する。

【0025】

ユーザホームネットワーク5は、サービスプロバイダ3から価格を付して送付されたコンテンツを入手し、コンテンツを復号、再生して利用するとともに課金

処理を実行する。課金処理により得られた課金情報は、ユーザホームネットワーク 5 が配送用鍵 K d を EMD サービスセンタ 1 から入手する際、EMD サービスセンタ 1 に送信される。

【0026】

図 2 は、EMD サービスセンタ 1 の機能の構成を示すブロック図である。サービスプロバイダ管理部 11 は、サービスプロバイダ 3 に利益分配の情報を供給するとともに、コンテンツプロバイダ 2 から供給されるコンテンツに付される情報（取扱方針）が暗号化されている場合、サービスプロバイダ 3 に配送用鍵 K d を送信する。コンテンツプロバイダ管理部 12 は、コンテンツプロバイダ 2 に配送用鍵 K d を送信するとともに、利益分配の情報を供給する。著作権管理部 13 は、ユーザホームネットワーク 5 のコンテンツの利用の実績を示す情報を、著作権を管理する団体、例えば、JASRAC (Japanese Society for Rights of Authors, Composers and Publishers: 日本音楽著作権協会) に送信する。鍵サーバ 14 は、配送用鍵 K d を記憶しており、コンテンツプロバイダ管理部 12、またはユーザ管理部 18 等を介して、配送用鍵 K d をコンテンツプロバイダ 2、またはユーザホームネットワーク 5 等に供給する。ユーザ管理部 18 は、ユーザホームネットワーク 5 のコンテンツの利用の実績を示す情報である課金情報、そのコンテンツに対応する価格情報、およびそのコンテンツに対応する取扱方針を入力し、経歴データ管理部 15 に記憶させる。

【0027】

EMD サービスセンタ 1 からコンテンツプロバイダ 2 およびユーザホームネットワーク 5 を構成するレシーバ 51（図 10 で後述する）への、配送用鍵 K d の定期的な送信の例について、図 3 乃至図 6 を参照に説明する。図 3 は、コンテンツプロバイダ 2 がコンテンツの提供を開始し、ユーザホームネットワーク 5 を構成するレシーバ 51 がコンテンツの利用を開始する、1998 年 1 月における、EMD サービスセンタ 1 が有する配送用鍵 K d、コンテンツプロバイダ 2 が有する配送用鍵 K d、およびレシーバ 51 が有する配送用鍵 K d を示す図である。

【0028】

図 3 の例において、配送用鍵 K d は、暦の月の初日から月の末日まで、使用可

能であり、たとえば、所定のビット数の乱数である” a a a a a a a a ” の値を有するバージョン1である配送用鍵K d は、1998年1月1日から1998年1月31日まで使用可能（すなわち、1998年1月1日から1998年1月31日の期間にサービスプロバイダ3がユーザホームネットワーク5に配布するコンテンツを暗号化するコンテンツ鍵K c o は、バージョン1である配送用鍵K d で暗号化されている）であり、所定のビット数の乱数である” b b b b b b b b ” の値を有するバージョン2である配送用鍵K d は、1998年2月1日から1998年2月28日まで使用可能（すなわち、その期間にサービスプロバイダ3がユーザホームネットワーク5に配布するコンテンツを暗号化するコンテンツ鍵K c o は、バージョン2である配送用鍵K d で暗号化されている）である。同様に、バージョン3である配送用鍵K d は、1998年3月中に使用可能であり、バージョン4である配送用鍵K d は、1998年4月中に使用可能であり、バージョン5である配送用鍵K d は、1998年5月中に使用可能であり、バージョン6である配送用鍵K d は、1998年6月中に使用可能である。

【0029】

コンテンツプロバイダ2がコンテンツの提供を開始するに先立ち、EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年1月から1998年6月まで利用可能な、バージョン1乃至バージョン6の6つの配送用鍵K d を送信し、コンテンツプロバイダ2は、6つの配送用鍵K d を受信し、記憶する。6月分の配送用鍵K d を記憶するのは、コンテンツプロバイダ2は、コンテンツを提供する前のコンテンツおよびコンテンツ鍵の暗号化などの準備に、所定の期間が必要だからである。

【0030】

また、レシーバ51がコンテンツの利用を開始するに先立ち、EMDサービスセンタ1は、レシーバ51に、1998年1月から1998年3月まで、利用可能なバージョン1乃至バージョン3である3つの配送用鍵K d を送信し、レシーバ51は、3つの配送用鍵K d を受信し、記憶する。3月分の配送用鍵K d を記憶するのは、レシーバ51が、EMDサービスセンタ1に接続できないなどのトラブルにより、コンテンツの利用が可能な契約期間にもかかわらずコンテンツが利用

できない等の事態を避けるためであり、また、EMDサービスセンタ1への接続の頻度を低くし、ユーザホームネットワーク5の負荷を低減するためである。

【0031】

1998年1月1日から1998年1月31日の期間には、バージョン1である配送用鍵Kdが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

【0032】

1998年2月1日における、EMDサービスセンタ1の配送用鍵Kdのコンテンツプロバイダ2、およびレシーバ51への送信を図4で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年2月から1998年7月まで利用可能な、バージョン2乃至バージョン7の6つの配送用鍵Kdを送信し、コンテンツプロバイダ2は、6つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、レシーバ51に、1998年2月から1998年4月まで、利用可能なバージョン2乃至バージョン4である3つの配送用鍵Kdを送信し、レシーバ51は、3つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、バージョン1である配送用鍵Kdをそのまま記憶する。これは、不測のトラブルが発生したとき、若しくは不正が発生し、または発見されたときに、過去に利用した配送用鍵Kdを利用できるようにするためである。

【0033】

1998年2月1日から1998年2月28日の期間には、バージョン2である配送用鍵Kdが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

【0034】

1998年3月1日における、EMDサービスセンタ1の配送用鍵Kdのコンテンツプロバイダ2、およびレシーバ51への送信を図5で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年3月から1998年8月まで利用可能な、バージョン3乃至バージョン8の6つの配送用鍵Kdを送信し

、コンテンツプロバイダ2は、6つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、レシーバ51に、1998年3月から1998年5月まで、利用可能なバージョン3乃至バージョン5である3つの配送用鍵Kdを送信し、レシーバ51は、3つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、バージョン1である配送用鍵Kdおよびバージョン2である配送用鍵Kdをそのまま記憶する。

【0035】

1998年3月1日から1998年3月31日の期間には、バージョン3である配送用鍵Kdが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

【0036】

1998年4月1日における、EMDサービスセンタ1の配送用鍵Kdのコンテンツプロバイダ2、およびレシーバ51への送信を図6で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年4月から1998年9月まで利用可能な、バージョン4乃至バージョン9の6つの配送用鍵Kdを送信し、コンテンツプロバイダ2は、6つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、レシーバ51に、1998年4月から1998年6月まで、利用可能なバージョン4乃至バージョン6である3つの配送用鍵Kdを送信し、レシーバ51は、3つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、バージョン1である配送用鍵Kd、バージョン2である配送用鍵Kd、およびバージョン3である配送用鍵Kdをそのまま記憶する。

【0037】

1998年4月1日から1998年4月30日の期間には、バージョン4である配送用鍵Kdが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

【0038】

このように、あらかじめ先の月の配送用鍵Kdを配布しておくことで、仮にユーザーが1, 2ヶ月まったくセンターにアクセスしていなくても、一応、コンテンツの買い取りが行え、時を見計らって、センターにアクセスして鍵を受信することができる。

【0039】

利益分配部16は、経歴データ管理部15から供給された、課金情報、価格情報、および取扱方針に基づき、EMDサービスセンタ1、コンテンツプロバイダ2、およびサービスプロバイダ3の利益を算出する。相互認証部17は、コンテンツプロバイダ2、サービスプロバイダ3、およびユーザホームネットワーク5の所定の機器と後述する相互認証を実行する。

【0040】

ユーザ管理部18は、ユーザ登録データベースを有し、ユーザホームネットワーク5の機器から登録の要求があったとき、ユーザ登録データベースを検索し、その記録内容に応じて、その機器を登録したり、または登録を拒絶する等の処理を実行する。ユーザホームネットワーク5がEMDサービスセンタ1と接続が可能な機能を有する複数の機器から構成されているとき、ユーザ管理部18は、登録が可能か否かの判定の処理の結果に対応して、決済をする機器を指定し、さらに、コンテンツの利用条件を規定した登録リストをユーザホームネットワーク5の所定の機器に送信する。

【0041】

図7に示すユーザ登録データベースの例は、ユーザホームネットワーク5の機器の機器固有の64ビットからなるID (Identification Data) を記録し、そのIDに対応して(すなわち、そのIDを有する機器毎に)、決済処理が可能か否か、登録が可能か否か、EMDサービスセンタ1と接続が可能か否か等の情報を記録する。

ユーザ登録データベースに記録された登録が可能か否かの情報は、決済機関(例えば、銀行)、またはサービスプロバイダ3などから供給される料金の未払い、不正処理等の情報を基に、所定の時間間隔で更新される。登録が不可と記録されたIDを有する機器の登録の要求に対して、ユーザ管理部18は、その登録を

拒否し、登録を拒否された機器は、以後、このシステムのコンテンツを利用できない。

【0042】

ユーザ登録データベースに記録された決済処理が可能か否かの情報は、その機器が、決済可能か否かを示す。ユーザホームネットワーク5が、コンテンツの再生またはコピーなどの利用が可能な複数の機器で構成されているとき、その中の決済処理が可能である1台の機器は、EMDサービスセンタ1に、ユーザホームネットワーク5のEMDサービスセンタ1に登録されている全ての機器の、課金情報、価格情報、および取扱方針を出力する。ユーザ登録データベースに記録されたEMDサービスセンタ1と接続が可能か否かの情報は、その機器が、EMDサービスセンタ1と接続が可能であるか否かを示し、接続できないと記録された機器は、ユーザホームネットワーク5の他の機器を介して、EMDサービスセンタ1に、課金情報等を出力する。

【0043】

また、ユーザ管理部18は、ユーザホームネットワーク5の機器から課金情報、価格情報、および取扱方針が供給され、その情報を経歴データ管理部15に出力し、さらに、所定の処理（タイミング）で、ユーザホームネットワーク5の機器に、配送用鍵Kdを供給する。

【0044】

課金請求部19は、経歴データ管理部15から供給された、課金情報、価格情報、および取扱方針に基づき、ユーザへの課金を算出し、その結果を、出納部20に供給する。出納部20は、ユーザ、コンテンツプロバイダ2、およびサービスプロバイダ3への出金、徴収すべき利用料金の金額を基に、図示せぬ外部の銀行等と通信し、決算処理を実行する。監査部21は、ユーザホームネットワーク5の機器から供給された課金情報、価格情報、および取扱方針の正当性（すなわち、不正をしていないか）を監査する。

【0045】

図8は、コンテンツプロバイダ2の機能の構成を示すブロック図である。コンテンツサーバ31は、ユーザに供給するコンテンツを記憶し、ウォーターマーク付

加部 32 に供給する。ウォーターマーク付加部 32 は、コンテンツサーバ 31 から供給されたコンテンツにウォーターマークを付加し、圧縮部 33 に供給する。圧縮部 33 は、ウォーターマーク付加部 32 から供給されたコンテンツを、ATRAC2 (Adaptive Transform Acoustic Coding 2) (商標) 等の方式で圧縮し、暗号化部 34 に供給する。暗号化部 34 は、圧縮部 33 で圧縮されたコンテンツを、乱数発生部 35 から供給された乱数を鍵 (以下、この乱数をコンテンツ鍵 K_c と称する) として、DES (Data Encryption Standard) などの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部 38 に出力する。

【0046】

乱数発生部 35 は、コンテンツ鍵 K_c となる所定のビット数の乱数を暗号化部 34 および暗号化部 36 に供給する。暗号化部 36 は、コンテンツ鍵 K_c を EMD サービスセンタ 1 から供給された配送用鍵 K_d を使用して、DES などの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部 38 に出力する。

【0047】

DES は、56 ビットの共通鍵を用い、平文の 64 ビットを 1 ブロックとして処理する暗号方式である。DES の処理は、平文を攪拌し、暗号文に変換する部分 (データ攪拌部) と、データ攪拌部で使用する鍵 (拡大鍵) を共通鍵から生成する部分 (鍵処理部) からなる。DES のすべてのアルゴリズムは公開されているので、ここでは、データ攪拌部の基本的な処理を簡単に説明する。

【0048】

まず、平文の 64 ビットは、上位 32 ビットの H_0 、および下位 32 ビットの L_0 に分割される。鍵処理部から供給された 48 ビットの拡大鍵 K_1 、および下位 32 ビットの L_0 を入力とし、下位 32 ビットの L_0 を攪拌した F 関数の出力が算出される。F 関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の 2 種類の基本変換から構成されている。次に、上位 32 ビットの H_0 と、F 関数の出力が排他的論理和され、その結果は L_1 とされる。 L_0 は、 H_1 とされる。

【0049】

上位 32 ビットの H_0 および下位 32 ビットの L_0 を基に、以上の処理を 16 回

繰り返し、得られた上位32ビットの H_{16} および下位32ビットの L_{16} が暗号文として出力される。復号は、暗号化に使用した共通鍵を用いて、上記の手順を逆にたどることで実現される。

【0050】

ポリシー記憶部37は、コンテンツの取扱方針（ポリシー）を記憶し、暗号化されるコンテンツに対応して、取扱方針をセキュアコンテナ作成部38に出力する。セキュアコンテナ作成部38は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵 K_{co} 、取扱方針、並びに暗号化されたコンテンツ、暗号化されたコンテンツ鍵 K_{co} 、および取扱方針のハッシュ値をとり作成された署名、さらにコンテンツプロバイダ2の公開鍵 K_{cp} を含む証明書から構成されるコンテンツプロバイダセキュアコンテナを作成し、サービスプロバイダ3に供給する。相互認証部39は、EMDサービスセンタ1から配送用鍵 K_d の供給を受けるのに先立ち、EMDサービスセンタ1と相互認証し、また、サービスプロバイダ3へのコンテンツプロバイダセキュアコンテナの送信に先立ち、サービスプロバイダ3と相互認証する。

【0051】

署名は、データまたは後述する証明書に付け、改竄のチェックおよび作成者認証をするためのデータであり、送信したいデータを基にハッシュ関数でハッシュ値をとり、これを公開鍵暗号の秘密鍵で暗号化して作成される。

【0052】

ハッシュ関数および署名の照合について説明する。ハッシュ関数は、送信したい所定のデータを入力とし、所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難である特徴を有する。

【0053】

署名とデータを受信した受信者は、署名を公開鍵暗号の公開鍵で復号し、その結果（ハッシュ値）を得る。さらに受信されたデータのハッシュ値が計算され、

計算されたハッシュ値と、署名を復号して得られたハッシュ値とが、等しいか否かが判定される。送信されたデータのハッシュ値と復号したハッシュ値が等しいと判定された場合、受信したデータは改竄されておらず、公開鍵に対応した秘密鍵を保持する送信者から送信されたデータであることがわかる。署名のハッシュ関数としては、MD4, MD5, SHA-1などが用いられる。

【0054】

次に公開鍵暗号について説明する。暗号化および復号で同一の鍵（共通鍵）を使用する共通鍵暗号方式に対し、公開鍵暗号方式は、暗号化に使用する鍵と復号するときの鍵が異なる。公開鍵暗号を用いる場合、鍵の一方を公開しても他方を秘密に保つことができ、公開しても良い鍵は、公開鍵と称され、他方の秘密に保つ鍵は、秘密鍵と称される。

【0055】

公開鍵暗号の中で代表的なRSA (Rivest-Shamir-Adleman) 暗号を、簡単に説明する。まず、2つの十分に大きな素数である p および q を求め、さらに p と q の積である n を求める。 $(p-1)$ と $(q-1)$ の最小公倍数 L を算出し、更に、3以上 L 未満で、かつ、 L と互いに素な数 e を求める（すなわち、 e と L を共通に割り切れる数は、1のみである）。

【0056】

次に、 L を法とする乗算に関する e の乗法逆元 d を求める。すなわち、 d 、 e 、および L の間には、 $ed=1 \bmod L$ が成立し、 d はユークリッドの互除法で算出できる。このとき、 n と e が公開鍵とされ、 p, q , および d が、秘密鍵とされる。

【0057】

暗号文 C は、平文 M から、式(1)の処理で算出される。

$$C=M^e \bmod n \quad (1)$$

【0058】

暗号文 C は、式(2)の処理で平文 M に、復号される。

$$M=C^d \bmod n \quad (2)$$

【0059】

証明は省略するが、RSA暗号で平文を暗号文に変換して、それが復号できるの

は、フェルマーの小定理に根拠をおいており、式(3)が成立するからである。

$$M = C^d = (M^e)^d = M^{ed} \pmod{n} \quad (3)$$

【0060】

秘密鍵 p と q を知っているならば、公開鍵 e から秘密鍵 d は算出できるが、公開鍵 n の素因数分解が計算量的に困難な程度に公開鍵 n の桁数を大きくすれば、公開鍵 n を知るだけでは、公開鍵 e から秘密鍵 d は計算できず、復号できない。以上のように、RSA暗号では、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

【0061】

また、公開鍵暗号の他の例である楕円曲線暗号についても、簡単に説明する。楕円曲線 $y^2 = x^3 + ax + b$ 上の、ある点を B とする。楕円曲線上の点の加算を定義し、 nB は、 B を n 回加算した結果を表す。同様に、減算も定義する。 B と nB から n を算出することは、困難であることが証明されている。 B と nB を公開鍵とし、 n を秘密鍵とする。乱数 r を用いて、暗号文 $C1$ および $C2$ は、平文 M から、公開鍵で式(4)および式(5)の処理で算出される。

$$C1 = M + rnB \quad (4)$$

$$C2 = rB \quad (5)$$

【0062】

暗号文 $C1$ および $C2$ は、式(6)の処理で平文 M に、復号される。

$$M = C1 - nC2 \quad (6)$$

【0063】

復号できるのは、秘密鍵 n を有するものだけである。以上のように、RSA暗号と同様に、楕円曲線暗号でも、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

【0064】

図9は、サービスプロバイダ3の機能の構成を示すブロック図である。コンテンツサーバ41は、コンテンツプロバイダ2から供給された、暗号化されているコンテンツを記憶し、セキュアコンテナ作成部44に供給する。値付け部42は、コンテンツに対応した取扱方針を基に、価格情報を作成し、セキュアコンテナ

作成部 44 に供給する。ポリシー記憶部 43 は、コンテンツプロバイダ 2 から供給された、コンテンツの取扱方針を記憶し、セキュアコンテナ作成部 44 に供給する。相互認証部 45 は、コンテンツプロバイダ 2 からコンテンツプロバイダセキュアコンテナの供給を受け取るのに先立ち、コンテンツプロバイダ 2 と相互認証し、また、ユーザホームネットワーク 5 へのサービスプロバイダセキュアコンテナの送信に先立ち、ユーザホームネットワーク 5 と相互認証する。また、コンテンツプロバイダ 2 が取扱方針を配送用鍵 K d で暗号化して供給する場合、相互認証部 45 は、EMDサービスセンタ 1 から配送用鍵 K d の供給を受け付けるのに先立ち、EMDサービスセンタ 1 と相互認証する。

【0065】

図 10 は、ユーザホームネットワーク 5 の構成を示すブロック図である。レシーバ 51 は、ネットワーク 4 を介して、サービスプロバイダ 3 からコンテンツを含んだサービスプロバイダセキュアコンテナを受信し、コンテンツを復号および伸張し、再生する。

【0066】

通信部 61 は、ネットワーク 4 を介してサービスプロバイダ 3、または EMD サービスセンタ 1 と通信し、所定の情報を受信し、または送信する。SAM (Secure Application Module) 62 は、サービスプロバイダ 3、または EMD サービスセンタ 1 と相互認証し、コンテンツの暗号を復号し、またはコンテンツを暗号化し、さらに配送用鍵 K d 等を記憶する。伸張部 63 は、コンテンツの暗号を復号し、ATRAC2 方式で伸張し、さらに所定のウォータマークをコンテンツに挿入する。IC (Integrated Circuit) カードインターフェース 64 は、SAM 62 からの信号を所定の形式に変更し、レシーバ 51 に装着された IC カード 55 に出力し、また、IC カード 55 からの信号を所定の形式に変更し、SAM 62 に出力する。

【0067】

サービスプロバイダ 3、または EMD サービスセンタ 1 と相互認証し、課金処理を実行し、コンテンツ鍵 K c o を復号および暗号化し、さらに使用許諾条件情報等の所定のデータを記憶する SAM 62 は、相互認証モジュール 71、課金モジュール 72、記憶モジュール 73、および復号／暗号化モジュール 74 から構成さ

れる。このSAM 62は、シングルチップの暗号処理専用ICで構成され、多層構造を有し、その内部のメモリセルはアルミニウム層等のダミー層に挟まれ、また、動作する電圧または周波数の幅が狭い等、外部から不正にデータが読み出し難い特性（耐タンパー性）を有する。

【0068】

相互認証モジュール71は、サービスプロバイダ3、またはEMDサービスセンタ1との相互認証を実行し、必要に応じて、一時鍵Ktemp（セッション鍵）を復号／暗号化モジュール74に供給する。課金処理モジュール72は、サービスプロバイダ3から受信したサービスプロバイダセキュアコンテナに含まれる取扱方針および価格情報（並びに、場合によっては、取扱制御情報）から、使用許諾条件情報および課金情報を生成し、記憶モジュール73またはHDD(Hard Disk Drive) 52に出力する。記憶モジュール73は、課金処理モジュール72または復号／暗号化モジュール74から供給された課金情報、および配送用鍵Kd等のデータを記憶し、他の機能ブロックが所定の処理を実行するとき、配送用鍵Kd等のデータを供給する。

【0069】

復号／暗号化モジュール74は、復号ユニット91、乱数発生ユニット92、および暗号化ユニット93から構成される。復号ユニット91は、暗号化されたコンテンツ鍵Kcoを配送用鍵Kdで復号し、暗号化ユニット93に出力する。乱数発生ユニット92は、所定の桁数の乱数を発生し、保存用鍵Ksaveとして暗号化ユニット93および記憶モジュール73に出力する。ただし、一度生成して保持している場合、その必要はない。暗号化ユニット93は、復号されたコンテンツ鍵Kcoを、再度、保存用鍵Ksaveで暗号化し、HDD 52に出力する。暗号化ユニット93は、コンテンツ鍵Kcoを伸張部63に送信するとき、コンテンツ鍵Kcoを一時鍵Ktempで暗号化する。

【0070】

コンテンツを復号し、伸張し、所定のウォーターマークを付加する伸張部63は、相互認証モジュール75、復号モジュール76、復号モジュール77、伸張モジュール78、およびウォーターマーク付加モジュール79から構成される。相互

認証モジュール75は、SAM62と相互認証し、一時鍵Ktempを復号モジュール76に出力する。復号モジュール76は、記憶モジュール73から出力され、一時鍵Ktempで暗号化されたコンテンツ鍵Kcoを一時鍵Ktempで復号し、復号モジュール77に出力する。復号モジュール77は、HDD52に記録されたコンテンツをコンテンツ鍵Kcoで復号し、伸張モジュール78に出力する。伸張モジュール78は、復号されたコンテンツを、更にATRAC2等の方式で伸張し、ウォーターマーク付加モジュール79に出力する。ウォーターマーク付加モジュール79は、コンテンツにレシーバ51を特定する所定のウォーターマークを挿入し、レコーダ53に出力したり、図示せぬスピーカに出力し、音楽を再生する。

【0071】

HDD52は、サービスプロバイダ3から供給されたコンテンツを記録する。装着された光ディスク（図示せず）にサービスプロバイダ3から供給されたコンテンツを記録し、再生するレコーダ53は、記録再生部65、SAM66、および伸張部67から構成される。記録再生部65は、光ディスクが装着され、その光ディスクにコンテンツを記録し、再生する。SAM66は、SAM62と同じ機能を有し、その説明は省略する。伸張部67は、伸張部63と同じ機能を有し、その説明は省略する。MD(Mini Disk:商標)ドライブ54は、装着された図示せぬMDにサービスプロバイダ3から供給されたコンテンツを記録し、再生する。

【0072】

ICカード55は、レシーバ51に装着され、記憶モジュール73に記憶された配送用鍵Kdおよび機器のIDなどの所定のデータを記憶する。例えば、新たなレシーバ51を購入し、今まで使用していたレシーバ51と入れ替えて使用する場合、まず、ユーザは、ICカード55に、今まで使用していたレシーバ51の記憶モジュール73に記憶されていた配送用鍵Kdなどの所定のデータを記憶させる

。次に、ユーザは、そのICカード55を新たなレシーバ51に装着し、そのレシーバ51を操作して、EMDサービスセンタ1のユーザ管理部18にその新たなレシーバ51を登録する。EMDサービスセンタ1のユーザ管理部18は、ICカード55に記憶されていたデータ（今まで使用していたレシーバ51のIDなど）を基

に、ユーザ管理部18が保持しているデータベースから、ユーザの氏名、使用料の払い込みに使用するクレジットカードの番号などのデータを検索し、そのデータを基に、登録の処理を実行するので、ユーザは、面倒なデータを入力する必要がない。ICカード55は、相互認証モジュール80および記憶モジュール81で構成される。相互認証モジュール80は、SAM62と相互認証する。記憶モジュール81は、ICカードインターフェース64を介して、SAM62から供給されたデータを記憶し、記憶したデータをSAM62に出力する。

【0073】

図11は、ユーザホームネットワーク5の他の構成例を示すブロック図である。この構成のレシーバ51およびレコーダ53は、図10に示した伸張部63および伸張部67を省略した構成を有する。その代わり、レコーダ53に接続されているデコーダ56が、伸張部63または伸張部67と同じ機能を有する。その他の構成は、図10における場合と同様である。

【0074】

コンテンツを復号し、伸張し、ウォーターマークを付加するデコーダ56は、相互認証モジュール101、復号モジュール102、復号モジュール103、伸張モジュール104、およびウォーターマーク付加モジュール105から構成される。相互認証モジュール101は、SAM62またはSAM66と相互認証し、一時鍵Ktempを復号モジュール102に出力する。復号モジュール102は、SAM62から出力され、一時鍵Ktempで暗号化されたコンテンツ鍵Kcoを一時鍵Ktempで復号し、復号モジュール103に出力する。復号モジュール103は、HDD52に記録されたコンテンツをコンテンツ鍵Kcoで復号し、伸張モジュール104に出力する。伸張モジュール104は、復号されたコンテンツを、更にATRAC2等の方式で伸張し、ウォーターマーク付加モジュール105に出力する。ウォーターマーク付加モジュール105は、コンテンツにデコーダ56を特定する所定のウォーターマークを挿入し、レコーダ53に出力したり、図示せぬスピーカに出力し、音楽を再生する。

【0075】

図12は、EMDサービスセンタ1、コンテンツプロバイダ2、サービスプロバ

イダ3、およびユーザホームネットワーク5の間で送受信される情報を説明する図である。コンテンツプロバイダ2は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Kco、取扱方針、および署名をコンテンツプロバイダセキュアコンテナ（その詳細は図13を参照して後述する）に格納し、さらにコンテンツプロバイダセキュアコンテナにコンテンツプロバイダ2の証明書（その詳細は図14を参照して後述する）を付して、サービスプロバイダ3に送信する。コンテンツプロバイダ2はまた、取扱方針、および署名にコンテンツプロバイダ2の証明書を付して、EMDサービスセンタ1に送信する。

【0076】

サービスプロバイダ3は、受信したコンテンツプロバイダセキュアコンテナに含まれる取扱方針を基に価格情報を生成し、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Kco、取扱方針、価格情報、および署名をサービスプロバイダセキュアコンテナ（その詳細は図15を参照して後述する）に格納し、さらにサービスプロバイダセキュアコンテナにサービスプロバイダ3の証明書（その詳細は図16を参照して後述する）を付して、ユーザホームネットワーク5に送信する。サービスプロバイダ3はまた、価格情報、および署名にサービスプロバイダ3の証明書を付して、EMDサービスセンタ1に送信する。

【0077】

ユーザホームネットワーク5は、受信したサービスプロバイダセキュアコンテナに含まれる取扱方針から使用許諾情報を生成し、使用許諾情報に沿って、コンテンツを利用する。ユーザホームネットワーク5において、コンテンツ鍵Kcoが復号されると、課金情報が生成される。課金情報は、所定のタイミングで、暗号化され、取扱方針と共に署名が付され、EMDサービスセンタ1に送信される。

【0078】

EMDサービスセンタ1は、課金情報および取扱方針を基に使用料金を算出し、またEMDサービスセンタ1、コンテンツプロバイダ2、およびサービスプロバイダ3それぞれの利益を算出する。EMDサービスセンタ1は、さらに、コンテンツプロバイダ2から受信した取扱方針、サービスプロバイダ3から受信した価格情報、並びにユーザホームネットワーク5から受信した課金情報および取扱方針を

比較し、サービスプロバイダ3またはユーザホームネットワーク5で取扱方針の改竄または不正な価格の付加等の不正がなかったか否かを監査する。

【0079】

図13は、コンテンツプロバイダセキュアコンテナを説明する図である。コンテンツプロバイダセキュアコンテナは、コンテンツ鍵 K_{co} で暗号化されたコンテンツ、配送用鍵 K_d で暗号化されたコンテンツ鍵 K_{co} 、取扱方針、および署名を含む。署名は、コンテンツ鍵 K_{co} で暗号化されたコンテンツ、配送用鍵 K_d で暗号化されたコンテンツ鍵 K_{co} 、および取扱方針にハッシュ関数を適用して生成されたハッシュ値を、コンテンツプロバイダ2の秘密鍵 K_{scp} で暗号化したデータである。

【0080】

図14は、コンテンツプロバイダ2の証明書を説明する図である。コンテンツプロバイダ2の証明書は、証明書のバージョン番号、認証局がコンテンツプロバイダ2に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、コンテンツプロバイダ2の名前、コンテンツプロバイダの公開鍵 K_{pcp} 、並びに署名を含む。署名は、証明書のバージョン番号、認証局がコンテンツプロバイダ2に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、コンテンツプロバイダ2の名前、並びにコンテンツプロバイダの公開鍵 K_{pcp} にハッシュ関数を適用して生成されたハッシュ値を、認証局の秘密鍵 K_{sca} で暗号化したデータである。

【0081】

図15は、サービスプロバイダセキュアコンテナを説明する図である。サービスプロバイダセキュアコンテナは、コンテンツ鍵 K_{co} で暗号化されたコンテンツ、配送用鍵 K_d で暗号化されたコンテンツ鍵 K_{co} 、取扱方針、価格情報、および署名を含む。署名は、コンテンツ鍵 K_{co} で暗号化されたコンテンツ、配送用鍵 K_d で暗号化されたコンテンツ鍵 K_{co} 、取扱方針、および価格情報にハッシュ関数を適用して生成されたハッシュ値を、サービスプロバイダ3の秘密鍵 K_{ssp} で暗号化したデータである。

【0082】

図16は、サービスプロバイダ3の証明書を説明する図である。サービスプロバイダ3の証明書は、証明書のバージョン番号、認証局がサービスプロバイダ3に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、サービスプロバイダ3の名前、サービスプロバイダの公開鍵 K_{psp} 、並びに署名を含む。署名は、証明書のバージョン番号、認証局がサービスプロバイダ3に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、サービスプロバイダ3の名前、サービスプロバイダの公開鍵 K_{psp} にハッシュ関数を適用して生成されたハッシュ値を、認証局の秘密鍵 K_{sca} で暗号化したデータである。

【0083】

図17は、取扱方針、価格情報、および使用許諾条件情報を示す図である。コンテンツプロバイダ2が有する取扱方針(図17(A))は、コンテンツ毎に用意され、ユーザホームネットワーク5が利用可能な利用内容を示す。例えば、図17(A)の取り扱い方針は、ユーザホームネットワーク5がそのコンテンツを再生およびマルチコピーすることは許可するが、シングルコピーは許可しないことを示す。

【0084】

図18は、シングルコピーおよびマルチコピーを説明する図である。マルチコピーは、使用許諾条件情報においてコピー許可が与えられているコンテンツに対し、その使用許諾条件を購入した場合において、そのコンテンツから、複数のコピーを作成することを言う。ただし、図18(A)に示すように、コピーを更にコピーすることはできない(許されない)。シングルコピーは、使用許諾条件情報においてコピー許可が与えられているコンテンツに対し、その使用許諾条件を購入した場合において、そのコンテンツから、ただ1つのコピーを作成することを言う。シングルコピーの場合も、図18(B)に示すように、コピーを更にコピーすることはできない(許されない)。

【0085】

サービスプロバイダ3は、図17(B)に示すように、コンテンツプロバイダ2からの取扱方針(図17(A))に価格情報を加える。例えば、図17(B)の価格情報は、そのコンテンツを再生して利用するときの料金が150円で、マルチコピーして利用するときの利用料金が80円であることを示す。図17には、例示しないが、シングルコピーの価格情報は、コピーの1回当たりの使用料金を表し、例えば、3回のコピーの利用では、シングルコピーの使用料金の3倍の料金を支払う。マルチコピーまたはシングルコピーが許可されるコンテンツは、使用許諾条件情報においてコピー許可が与えられているコンテンツに対し、その使用許諾条件を購入した場合における、そのコンテンツに限られる。

【0086】

ユーザホームネットワーク5は、サービスプロバイダ3から供給される取扱方針が示すコンテンツの利用可能な利用内容(図17(B))から、ユーザが選択した、利用内容を示す使用許諾条件情報(図17(C))を記憶する。例えば、図17(C)の使用許諾条件情報は、そのコンテンツを再生して使用することができ、シングルコピーおよびマルチコピーができないことを示す。

【0087】

図19は、図17の例と比較してコンテンツプロバイダ2が取扱方針に利益分配の情報を加え、サービスプロバイダ3が価格情報に利益分配の情報を加える場合の、取扱方針および価格情報を説明する図である。図17に示す例に対して、図19の例では、コンテンツプロバイダ2の利益が、コンテンツを再生して利用するとき70円で、マルチコピーして利用するとき40円であることを示す情報が、追加されている(図19(A))。更に、利益分配情報として、サービスプロバイダ3の利益が、コンテンツを再生して利用するとき60円で、マルチコピーして利用するとき30円であることが、追加されている(図19(B))。価格は、図17(A)における場合と同様に、再生が150円、マルチコピーが40円とされている。価格(例えば150円)からコンテンツプロバイダ2の利益(例えば70円)およびサービスプロバイダ3の利益(例えば60円)を差し引いた金額(例えば20円)が、EMDサービスセンタ1の利益である。EMDサービス

センタ1は、ユーザホームネットワーク5のコンテンツの利用結果を示す課金情報（図19（C））とともに、ユーザホームネットワーク5を介して、取扱方針、利益分配率、および価格情報を得ることで、コンテンツプロバイダ2、サービスプロバイダ3、およびEMDサービスセンタ1のそれぞれの利益を算出できる。

【0088】

図20は、コンテンツの再生の利用に、複数の形態が設定されているときの取扱方針、価格情報、および使用許諾条件情報を説明する図である。図20（A）の例では、サービスプロバイダ3において、取扱方針および価格情報として、コンテンツの再生利用に、制限のない再生、回数制限（この例の場合、5回）のある再生、および期日制限（この例の場合、1998年12月31日まで）のある再生が設定されている。ユーザが、5回の回数制限のある再生を選択して、コンテンツを利用する場合、コンテンツを受け取り、まだ1度も再生していない状態では、図20（B）に示すように、ユーザホームネットワーク5の使用許諾条件情報の回数制限に対応する値には、“5”が記録されている。この回数制限に対応する値は、ユーザホームネットワーク5において、コンテンツが再生（利用）される度にデクリメントされ、例えば、3回再生された後、その値は、図20（C）に示すように“2”とされる。回数制限に対応する値が、“0”となった場合、ユーザホームネットワーク5は、それ以上、そのコンテンツを再生して利用することができない。

【0089】

図21は、EMDサービスセンタ1、コンテンツプロバイダ2、サービスプロバイダ3、およびユーザホームネットワーク5の間で送受信される情報の他の例を説明する図である。図12に示した例に対して、図21の例では、サービスプロバイダ3は、コンテンツプロバイダ2からの取扱方針を基に取扱制御情報を作成する。取扱制御情報は、コンテンツなどと共にサービスプロバイダセキュアコンテナに格納され、ユーザホームネットワーク5に送信され、EMDサービスセンタ1にも送信される。取扱制御情報は、更に、課金情報および取扱方針と共にユーザホームネットワーク5からEMDサービスセンタ1に送信される。

【0090】

図22は、図21の例の場合のサービスプロバイダセキュアコンテナを説明する図である。サービスプロバイダセキュアコンテナは、コンテンツ鍵K_{co}で暗号化されたコンテンツ、配送用鍵K_dで暗号化されたコンテンツ鍵K_{co}、取扱方針、取扱制御情報、価格情報、および署名を含む。署名は、コンテンツ鍵K_{co}で暗号化されたコンテンツ、配送用鍵K_dで暗号化されたコンテンツ鍵K_{co}、取扱方針、取扱制御情報、および価格情報にハッシュ関数を適用して生成されたハッシュ値を、サービスプロバイダ3の秘密鍵K_{ssp}で暗号化したデータである。

【0091】

図23は、図21の例の場合における、取扱方針、取扱制御情報、価格情報、及び使用許諾条件の構成を示す図である。図23に示す例の場合、コンテンツプロバイダ2の取扱方針（図23（A））は、そのまま価格情報を付しても、取扱方針と対比して価格情報を参照できる形式を有しない。そこで、サービスプロバイダ3は、その取扱方針を基に、価格情報と対比して価格情報を参照できる形式を有する取扱制御情報を生成し、それに価格情報を付して、ユーザホームネットワーク5に送信する（図23（B））。ユーザホームネットワークでは、送信を受けた情報から使用許諾条件情報（図23（C））を生成する。図23のコンテンツプロバイダ2は、図12の場合に比較し、より小さいデータ量の取扱方針を記録すればよい利点がある。

【0092】

図24は、EMDサービスセンタ1、コンテンツプロバイダ2、サービスプロバイダ3、およびユーザホームネットワーク5の間で送受信されるコンテンツおよびコンテンツに付随する情報のさらに他の構成を説明する図である。図21に示した例に対して、図24の例では、取扱方針、取扱制御情報、価格情報、および課金情報は、公開鍵暗号により暗号化され、送信される。図24のシステムは、図21の例の場合に比較して、システムの外部からの攻撃に対し、安全性が向上する。

【0093】

図25は、図24の例の場合のコンテンツプロバイダセキュアコンテナを説明する図である。コンテンツプロバイダセキュアコンテナは、コンテンツ鍵K_{co}で暗号化されたコンテンツ、配送用鍵K_dで暗号化されたコンテンツ鍵K_{co}、配送用鍵K_dで暗号化された取扱方針、および署名を含む。署名は、コンテンツ鍵K_{co}で暗号化されたコンテンツ、配送用鍵K_dで暗号化されたコンテンツ鍵K_{co}、および配送用鍵K_dで暗号化された取扱方針にハッシュ関数を適用して生成されたハッシュ値を、コンテンツプロバイダ2の秘密鍵K_{scp}で暗号化したデータである。

【0094】

図26は、図24の例の場合のサービスプロバイダセキュアコンテナを説明する図である。サービスプロバイダセキュアコンテナは、コンテンツ鍵K_{co}で暗号化されたコンテンツ、配送用鍵K_dで暗号化されたコンテンツ鍵K_{co}、配送用鍵K_dで暗号化された取扱方針、配送用鍵K_dで暗号化された取扱制御情報、配送用鍵K_dで暗号化された価格情報、および署名を含む。署名は、コンテンツ鍵K_{co}で暗号化されたコンテンツ、配送用鍵K_dで暗号化されたコンテンツ鍵K_{co}、配送用鍵K_dで暗号化された取扱方針、配送用鍵K_dで暗号化された取扱制御情報、および配送用鍵K_dで暗号化された価格情報にハッシュ関数を適用して生成されたハッシュ値を、サービスプロバイダ3の秘密鍵K_{ssp}で暗号化したデータである。

【0095】

図27は、EMDサービスセンタ1が、ユーザホームネットワーク5から課金情報を受信するときの動作を説明する図である。ユーザホームネットワーク5と相互認証した後、ユーザ管理部18は、一時鍵K_{temp}を共有化し、鍵サーバ14からの配送用鍵K_dをこの鍵で暗号化しユーザホームネットワーク5に送信する。ユーザホームネットワーク5は、受信した配送用鍵K_dを共有化した一時鍵K_{temp}で復号した後、配送用鍵K_dを必要に応じて更新する。また、共有化した一時鍵K_{temp}を用いて課金情報、および取扱方針等を暗号化し、EMDサービスセンタ1に送信する。ユーザ管理部18はこれを受信する。ユーザ管理部

18は、受信した課金情報、および取扱方針等を共有化した一時鍵K t e m pで復号化した後、経歴データ管理部15および課金請求部19に送信する。経歴データ管理部15は決済を実行すると判定した場合、受信した課金情報を利益分配部16に送信し、さらに、受信した課金情報および取扱方針等を課金請求部19に送信する。利益分配部16は、コンテンツプロバイダ2、サービスプロバイダ3、およびEMDサービスセンタ1自身に対する請求金額および支払金額を算出する。課金請求部19は、ユーザの支払い金額を算出し、その情報を出納部20に送信する。出納部20は、図示せぬ外部の銀行等と通信し、決算処理を実行する。その際、ユーザの料金の未払い等の情報があれば、それらの情報は、課金請求部19およびユーザ管理部18に送信され、以後のユーザの登録処理時、または配送用鍵K dの送信処理時に参照される。

【0096】

図28は、EMDサービスセンタ1の利益分配処理の動作を説明する図である。経歴データ管理部15は、ユーザのコンテンツの使用実績を示す課金情報、取扱方針、および価格データを利益分配部16に送信する。利益分配部16は、これらの情報を基に、コンテンツプロバイダ2、サービスプロバイダ3、およびEMDサービスセンタ1それぞれの利益を算出し、その結果をサービスプロバイダ管理部11、コンテンツプロバイダ管理部12、出納部20、および著作権管理部13に送信する。出納部20は、図示せぬ外部の銀行等と通信し、決算処理を実行する。サービスプロバイダ管理部11は、サービスプロバイダ3の利益の情報をサービスプロバイダ3に送信する。コンテンツプロバイダ管理部12は、コンテンツプロバイダ2の利益の情報をコンテンツプロバイダ2に送信する。監査部21は、ユーザホームネットワーク5の機器から供給された課金情報、価格情報、および取扱方針の正当性を監査する。

【0097】

図29は、EMDサービスセンタ1の、コンテンツの利用実績の情報をJASRACに送信する処理の動作を説明する図である。経歴データ管理部15は、ユーザのコンテンツの使用実績を示す課金情報を著作権管理部13および利益分配部16に送信する。利益分配部16は、JASRACに対する請求金額および支払金額を算出し

、その情報を出納部20に送信する。出納部20は、図示せぬ外部の銀行等と通信し、決算処理を実行する。著作権管理部13は、ユーザのコンテンツの使用実績をJASRACに送信する。

【0098】

次に、EMDシステムの処理について説明する。図30は、このシステムのコンテンツの配布および再生の処理を説明するフローチャートである。ステップS11において、EMDサービスセンタ1のコンテンツプロバイダ管理部12は、コンテンツプロバイダ2に配送用鍵Kdを送信し、コンテンツプロバイダ2がこれを受信する。その処理の詳細は、図32のフローチャートを参照して後述する。ステップS12において、ユーザは、ユーザホームネットワーク5の機器（例えば、図10のレシーバ51）を操作し、ユーザホームネットワーク5の機器をEMDサービスセンタ1のユーザ管理部18に登録する。この登録処理の詳細は、図36のフローチャートを参照して後述する。ステップS13において、EMDサービスセンタ1のユーザ管理部18は、ユーザホームネットワーク5と、図33乃至図35に示したように相互認証した後、ユーザホームネットワーク5の機器に、配送用鍵Kdを送信する。ユーザホームネットワーク5はこの鍵を受信する。この処理の詳細は、図45のフローチャートを参照して説明する。

【0099】

ステップS14において、コンテンツプロバイダ2のセキュアコンテナ作成部38は、サービスプロバイダ3にコンテンツプロバイダセキュアコンテナを送信する。この送信処理の詳細は、図47のフローチャートを参照して後述する。ステップS15において、サービスプロバイダ3のセキュアコンテナ作成部44は、ユーザホームネットワーク5からの要求に応じて、ネットワーク4を介して、ユーザホームネットワーク5にサービスプロバイダセキュアコンテナを送信する。この送信処理の詳細は、図49のフローチャートを参照して後述する。ステップS16において、ユーザホームネットワーク5の課金モジュール72は、課金処理を実行する。課金処理の詳細は、図51のフローチャートを参照して後述する。ステップS17において、ユーザは、ユーザホームネットワーク5の機器でコンテンツを再生する。再生処理の詳細は、図52のフローチャートを参照して

後述する。

【0100】

一方、コンテンツプロバイダ2が、取扱方針を暗号化して送信する場合の処理は、図31のフローチャートで示すようになる。ステップS21において、EMDサービスセンタ1のコンテンツプロバイダ管理部12は、コンテンツプロバイダ2に配送用鍵Kdを送信する。ステップS22において、EMDサービスセンタ1のサービスプロバイダ管理部11は、サービスプロバイダ3に配送用鍵Kdを送信する。それ以降のステップS23乃至ステップS28の処理は、図30のステップS12乃至ステップS17の処理と同様の処理であり、その説明は省略する。

【0101】

図32は、図30のステップS11および図31のステップS21に対応する、EMDサービスセンタ1がコンテンツプロバイダ2へ配送用鍵Kdを送信し、コンテンツプロバイダ2がこれを受信する処理の詳細を説明するフローチャートである。ステップS31において、EMDサービスセンタ1の相互認証部17は、コンテンツプロバイダ2の相互認証部39と相互認証する。この相互認証処理の詳細は、図33を参照して後述する。相互認証処理により、コンテンツプロバイダ2が、正当なプロバイダであることが確認されたとき、ステップS32において、コンテンツプロバイダ2の暗号化部34および暗号化部36は、EMDサービスセンタ1のコンテンツプロバイダ管理部12から送信された配送用鍵Kdを受信する。ステップS33において、コンテンツプロバイダ2の暗号化部34は、受信した配送用鍵Kdを記憶する。

【0102】

このように、コンテンツプロバイダ2は、EMDサービスセンタ1から配送用鍵Kdを受け取る。同様に、図31に示すフローチャートの処理を行う例の場合、コンテンツプロバイダ2以外に、サービスプロバイダ3も、図32と同様の処理で、EMDサービスセンタ1から配送用鍵Kdを受け取る。

【0103】

次に、図32のステップS31における、いわゆるなりすましがいないことを確

認する相互認証の処理について、1つの共通鍵を用いる（図33）、2つの共通鍵を用いる（図34）、および公開鍵暗号を用いる（図35）を例として説明する。

【0104】

図33は、1つの共通鍵で、共通鍵暗号であるDESを用いる、コンテンツプロバイダ2の相互認証部39とEMDサービスセンタ1の相互認証部17との相互認証の動作を説明するフローチャートである。ステップS41において、コンテンツプロバイダ2の相互認証部39は、64ビットの乱数R1を生成する（乱数生成部35が生成するようにしてもよい）。ステップS42において、コンテンツプロバイダ2の相互認証部39は、DESを用いて乱数R1を、予め記憶している共通鍵Kcで暗号化する（暗号化部36で暗号化するようにしてもよい）。ステップS43において、コンテンツプロバイダ2の相互認証部39は、暗号化された乱数R1をEMDサービスセンタ1の相互認証部17に送信する。

【0105】

ステップS44において、EMDサービスセンタ1の相互認証部17は、受信した乱数R1を予め記憶している共通鍵Kcで復号する。ステップS45において、EMDサービスセンタ1の相互認証部17は、32ビットの乱数R2を生成する。ステップS46において、EMDサービスセンタ1の相互認証部17は、復号した64ビットの乱数R1の下位32ビットを乱数R2で入れ替え、接続 $R1_H \parallel R2$ を生成する。なお、ここで $R1_H$ は、R1の上位ビットを表し、 $A \parallel B$ は、AとBの接続（nビットのAの下位に、mビットのBを結合して、 $(n+m)$ ビットとしたもの）を表す。ステップS47において、EMDサービスセンタ1の相互認証部17は、DESを用いて $R1_H \parallel R2$ を共通鍵Kcで暗号化する。ステップS48において、EMDサービスセンタ1の相互認証部17は、暗号化した $R1_H \parallel R2$ をコンテンツプロバイダ2に送信する。

【0106】

ステップS49において、コンテンツプロバイダ2の相互認証部39は、受信した $R1_H \parallel R2$ を共通鍵Kcで復号する。ステップS50において、コンテンツプロバイダ2の相互認証部39は、復号した $R1_H \parallel R2$ の上位32ビット $R1_H$

を調べ、ステップS41で生成した、乱数R1の上位32ビット $R1_H$ と一致すれば、EMDサービスセンタ1が正当なセンタであることを認証する。生成した乱数 $R1_H$ と、受信した $R1_H$ が一致しないとき、処理は終了される。両者が一致するとき、ステップS51において、コンテンツプロバイダ2の相互認証部39は、32ビットの乱数R3を生成する。ステップS52において、コンテンツプロバイダ2の相互認証部39は、受信し、復号した32ビットの乱数R2を上位に設定し、生成した乱数R3をその下位に設定し、接続 $R2 \parallel R3$ とする。ステップS53において、コンテンツプロバイダ2の相互認証部39は、DESを用いて接続 $R2 \parallel R3$ を共通鍵Kcで暗号化する。ステップS54において、コンテンツプロバイダ2の相互認証部39は、暗号化された接続 $R2 \parallel R3$ をEMDサービスセンタ1の相互認証部17に送信する。

【0107】

ステップS55において、EMDサービスセンタ1の相互認証部17は、受信した接続 $R2 \parallel R3$ を共通鍵Kcで復号する。ステップS56において、EMDサービスセンタ1の相互認証部17は、復号した接続 $R2 \parallel R3$ の上位32ビットを調べ、乱数R2と一致すれば、コンテンツプロバイダ2を正当なプロバイダとして認証し、一致しなければ、不正なプロバイダとして、処理を終了する。

【0108】

図34は、2つの共通鍵Kc1, Kc2で、共通鍵暗号であるDESを用いる、コンテンツプロバイダ2の相互認証部39とEMDサービスセンタ1の相互認証部17との相互認証の動作を説明するフローチャートである。ステップS61において、コンテンツプロバイダ2の相互認証部39は、64ビットの乱数R1を生成する。ステップS62において、コンテンツプロバイダ2の相互認証部39は、DESを用いて乱数R1を予め記憶している共通鍵Kc1で暗号化する。ステップS63において、コンテンツプロバイダ2の相互認証部39は、暗号化された乱数R1をEMDサービスセンタ1に送信する。

【0109】

ステップS64において、EMDサービスセンタ1の相互認証部17は、受信した乱数R1を予め記憶している共通鍵Kc1で復号する。ステップS65におい

て、EMDサービスセンタ1の相互認証部17は、乱数R1を予め記憶している共通鍵Kc2で暗号化する。ステップS66において、EMDサービスセンタ1の相互認証部17は、64ビットの乱数R2を生成する。ステップS67において、EMDサービスセンタ1の相互認証部17は、乱数R2を共通鍵Kc2で暗号化する。ステップS68において、EMDサービスセンタ1の相互認証部17は、暗号化された乱数R1および乱数R2をコンテンツプロバイダ2の相互認証部39に送信する。

【0110】

ステップS69において、コンテンツプロバイダ2の相互認証部39は、受信した乱数R1および乱数R2を予め記憶している共通鍵Kc2で復号する。ステップS70において、コンテンツプロバイダ2の相互認証部39は、復号した乱数R1を調べ、ステップS61で生成した乱数R1（暗号化する前の乱数R1）と一致すれば、EMDサービスセンタ1を適正なセンタとして認証し、一致しなければ、不正なセンタであるとして、処理を終了する。ステップS71において、コンテンツプロバイダ2の相互認証部39は、復号して得た乱数R2を共通鍵Kc1で暗号化する。ステップS72において、コンテンツプロバイダ2の相互認証部39は、暗号化された乱数R2をEMDサービスセンタ1に送信する。

【0111】

ステップS73において、EMDサービスセンタ1の相互認証部17は、受信した乱数R2を共通鍵Kc1で復号する。ステップS74において、EMDサービスセンタ1の相互認証部17は、復号した乱数R2が、ステップS66で生成した乱数R2（暗号化する前の乱数R2）と一致すれば、コンテンツプロバイダ2を適正なプロバイダとして認証し、一致しなければ、不正なプロバイダであるとして処理を終了する。

【0112】

図35は、公開鍵暗号である、160ビット長の楕円曲線暗号を用いる、コンテンツプロバイダ2の相互認証部39とEMDサービスセンタ1の相互認証部17との相互認証の動作を説明するフローチャートである。ステップS81において、コンテンツプロバイダ2の相互認証部39は、64ビットの乱数R1を生成す

る。ステップ S 8 2 において、コンテンツプロバイダ 2 の相互認証部 3 9 は、自分自身の公開鍵 $K_{p c p}$ を含む証明書（認証局から予め取得しておいたもの）と、乱数 $R 1$ を EMD サービスセンタ 1 の相互認証部 1 7 に送信する。

【0113】

ステップ S 8 3 において、EMD サービスセンタ 1 の相互認証部 1 7 は、受信した証明書の署名（認証局の秘密鍵 $K_{s c a}$ で暗号化されている）を、予め取得しておいた認証局の公開鍵 $K_{p c a}$ で復号し、コンテンツプロバイダ 2 の公開鍵 $K_{p c p}$ とコンテンツプロバイダ 2 の名前のハッシュ値を取り出すとともに、証明書に平文のまま格納されているコンテンツプロバイダ 2 の公開鍵 $K_{p c p}$ およびコンテンツプロバイダ 2 の名前を取り出す。証明書が認証局が発行した適正なものであれば、証明書の署名を復号することが可能であり、復号して得られた公開鍵 $K_{p c p}$ およびコンテンツプロバイダ 2 の名前のハッシュ値は、平文のまま証明書に格納されていたコンテンツプロバイダ 2 の公開鍵 $K_{p c p}$ およびコンテンツプロバイダ 2 の名前にハッシュ関数を適用して得られたハッシュ値と一致する。これにより、公開鍵 $K_{p c p}$ が改竄されたものでない適正なものであることが認証される。署名を復号出来なかったり、できたとしてもハッシュ値が一致しないときには、適正な公開鍵でないか、適正なプロバイダでないことになる。この時処理は終了される。

【0114】

適正な認証結果が得られたとき、ステップ S 8 4 において、EMD サービスセンタ 1 の相互認証部 1 7 は、64 ビットの乱数 $R 2$ を生成する。ステップ S 8 5 において、EMD サービスセンタ 1 の相互認証部 1 7 は、乱数 $R 1$ および乱数 $R 2$ の接続 $R 1 \parallel R 2$ を生成する。ステップ S 8 6 において、EMD サービスセンタ 1 の相互認証部 1 7 は、接続 $R 1 \parallel R 2$ を自分自身の秘密鍵 $K_{s e s c}$ で暗号化する。ステップ S 8 7 において、EMD サービスセンタ 1 の相互認証部 1 7 は、接続 $R 1 \parallel R 2$ を、ステップ S 8 3 で取得したコンテンツプロバイダ 2 の公開鍵 $K_{p c p}$ で暗号化する。ステップ S 8 8 において、EMD サービスセンタ 1 の相互認証部 1 7 は、秘密鍵 $K_{s e s c}$ で暗号化された接続 $R 1 \parallel R 2$ 、公開鍵 $K_{p c p}$ で暗号化された接続 $R 1 \parallel R 2$ 、および自分自身の公開鍵 $K_{p e s c}$ を含む証明書（

認証局から予め取得しておいたもの) をコンテンツプロバイダ 2 の相互認証部 39 に送信する。

【0115】

ステップ S 89 において、コンテンツプロバイダ 2 の相互認証部 39 は、受信した証明書の署名を予め取得しておいた認証局の公開鍵 K_{pca} で復号し、正しければ証明書から公開鍵 K_{pesc} を取り出す。この場合の処理は、ステップ S 83 における場合と同様であるので、その説明は省略する。ステップ S 90 において、コンテンツプロバイダ 2 の相互認証部 39 は、EMD サービスセンタ 1 の秘密鍵 K_{sesc} で暗号化されている接続 $R1 \parallel R2$ を、ステップ S 89 で取得した公開鍵 K_{pesc} で復号する。ステップ S 91 において、コンテンツプロバイダ 2 の相互認証部 39 は、自分自身の公開鍵 K_{pcp} で暗号化されている接続 $R1 \parallel R2$ を、自分自身の秘密鍵 K_{scp} で復号する。ステップ S 92 において、コンテンツプロバイダ 2 の相互認証部 39 は、ステップ S 90 で復号された接続 $R1 \parallel R2$ と、ステップ S 91 で復号された接続 $R1 \parallel R2$ を比較し、一致すれば EMD サービスセンタ 1 を適正なものとして認証し、一致しなければ、不適正なものとして、処理を終了する。

【0116】

適正な認証結果が得られたとき、ステップ S 93 において、コンテンツプロバイダ 2 の相互認証部 39 は、64 ビットの乱数 $R3$ を生成する。ステップ S 94 において、コンテンツプロバイダ 2 の相互認証部 39 は、ステップ S 90 で取得した乱数 $R2$ および生成した乱数 $R3$ の接続 $R2 \parallel R3$ を生成する。ステップ S 95 において、コンテンツプロバイダ 2 の相互認証部 39 は、接続 $R2 \parallel R3$ を、ステップ S 89 で取得した公開鍵 K_{pesc} で暗号化する。ステップ S 96 において、コンテンツプロバイダ 2 の相互認証部 39 は、暗号化した接続 $R2 \parallel R3$ を EMD サービスセンタ 1 の相互認証部 17 に送信する。

【0117】

ステップ S 97 において、EMD サービスセンタ 1 の相互認証部 17 は、暗号化された接続 $R2 \parallel R3$ を自分自身の秘密鍵 K_{sesc} で復号する。ステップ S 98 において、EMD サービスセンタ 1 の相互認証部 17 は、復号した乱数 $R2$ が、

ステップS 84で生成した乱数R 2（暗号化する前の乱数R 2）と一致すれば、コンテンツプロバイダ2を適正なプロバイダとして認証し、一致しなければ、不適正なプロバイダとして、処理を終了する。

【0118】

以上のように、EMDサービスセンタ1の相互認証部17とコンテンツプロバイダ2の相互認証部39は、相互認証する。相互認証に利用された乱数は、その相互認証に続く処理にだけ有効な一時鍵K t e m pとして利用される。

【0119】

図36は、図30のステップS12および図31のステップS23に対応する、レシーバ51がEMDサービスセンタ1のユーザ管理部18に登録する処理を説明するフローチャートである。ステップS101において、レシーバ51のSAM62は、ICカードインターフェース64の出力から、レシーバ51にバックアップ用のICカード55が装着されているか否かを判定し、バックアップ用のICカード55が装着されていると判定された場合（例えば、レシーバ51が新たなレシーバ51に変更され、元のレシーバ51のデータを、新たなレシーバ51に引き継ぐために、元のレシーバ51のデータをバックアップ用のICカード55にバックアップさせている場合）、ステップS102に進み、ICカード55に記憶されているバックアップデータの読み込み処理を実行する。この処理の詳細は、図41のフローチャートを参照して後述する。勿論、この読み込み処理が実行されるためには、その前に、ICカード55に、バックアップデータを記憶させる必要があるが、その処理は、図39を参照して後述する。

【0120】

ステップS101において、バックアップ用のICカード55が装着されていないと判定された場合、手続は、ステップS102をスキップし、ステップS103に進む。ステップS103において、SAM62の相互認証モジュール71は、EMDサービスセンタ1の相互認証部17と相互認証し、SAM62は、証明書をEMDサービスセンタ1のユーザ管理部18に送信する。この認証処理は、図33乃至図35を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS103で、SAM62がEMDサービスセンタ1のユーザ管理部18に送信する

証明書は、図 37 に示すデータを含む。SAM 62 が送信する証明書は、図 14 に示すコンテンツプロバイダ 2 の証明書とほぼ同様の構成を有するが、更に、他の SAM に従属するか否かを示すデータを含んでいる。ステップ S 104 において、SAM 62 は、通信部 61 を介して、一時鍵 K_{temp} で暗号化した、ユーザの銀行等の決済機関の情報等を EMD サービスセンタ 1 のユーザ管理部 18 に送信する。

【0121】

ステップ S 105 において、EMD サービスセンタ 1 のユーザ管理部 18 は、受信した SAM 62 の ID を基に、図 7 に示したユーザ登録データベースを検索する。ステップ S 106 において、EMD サービスセンタ 1 のユーザ管理部 18 は、受信した ID を有する SAM 62 の登録が可能であるか否かを判定し、受信した ID を有する SAM 62 の登録が可能であると判定された場合、ステップ S 107 に進み、受信した ID を有する SAM 62 が、新規登録であるか否かを判定する。ステップ S 107 において、受信した ID を有する SAM 62 が、新規登録ではないと判定された場合、手続は、ステップ S 108 に進む。

【0122】

ステップ S 108 において、EMD サービスセンタ 1 のユーザ管理部 18 は、更新登録を実行し、受信した ID を基にユーザ登録データベースを検索し、登録リストを作成する。この登録リストは、例えば、図 38 に示す構造を有し、機器の SAM の ID に対応して、EMD サービスセンタ 1 のユーザ管理部 18 が登録を拒絶したか否かを示す登録拒絶フラグ、従属する機器である場合のコンテンツ鍵 K_{co} の利用条件を示すステータスフラグ、従属する機器であるか否かを示すコンディションフラグ、並びに登録拒絶フラグ、ステータスフラグ、およびコンディションフラグにハッシュ関数を適用して生成したハッシュ値を EMD サービスセンタ 1 の秘密鍵 K_{sec} で暗号化した署名から構成される。

【0123】

機器の SAM の ID は、機器の固有の 64 ビットからなる ID を示す（図 38 では、16 進数で示す）。登録拒絶フラグの“1”は、EMD サービスセンタ 1 のユーザ管理部 18 が対応する ID を有する機器を登録したことを示し、登録拒絶フラグの“0”は、MD サービスセンタ 1 のユーザ管理部 18 が対応する ID を有する機器の

登録を拒絶したことを示す。

【0124】

ステータスフラグのMSB(Most Significant Bit)の”1”は、対応するIDを有する子の機器（例えばレコーダ53）が従属した親の機器（例えばレシーバ51）からコンテンツ鍵K c oをもらえることを示し、ステータスフラグのMSBの”0”は、対応するIDを有する子の機器が従属した親の機器からコンテンツ鍵K c oをもらえないことを示している。ステータスフラグの上位から2ビット目の”1”は、対応するIDを有する子の機器が従属した親の機器から、親の機器の保存用鍵K s a v eで暗号化されたコンテンツ鍵K c oをもらえることを示す。ステータスフラグの上位から3ビット目の”1”は、対応するIDを有する子の機器が従属した親の機器から、配送用鍵K dで暗号化されたコンテンツ鍵K c oをもらえることを示す。ステータスフラグのLSB(Least Significant Bit)の”1”は、従属した親の機器が配送用鍵K dで暗号化したコンテンツ鍵K c oを購入し、対応するIDを有する子の機器に、一時鍵K t e m pで暗号化してコンテンツ鍵K c oを渡すことを示す。

【0125】

コンディションフラグの”0”は、対応するIDを有する機器がEMDサービスセンタ1のユーザ管理部18と直接通信が出来る（すなわち、例えばレシーバ51のような親の機器である）ことを示し、コンディションフラグの”1”は、対応するIDを有する機器がEMDサービスセンタ1のユーザ管理部18と直接通信が出来ない（すなわち、例えばレコーダ53のような子の機器である）ことを示す。コンディションフラグが”0”のとき、ステータスフラグは常に”0000”に設定される。

【0126】

ステップS109において、EMDサービスセンタ1のユーザ管理部18は、相互認証部17から供給された一時鍵K t e m pで暗号化した、鍵サーバ14から供給された配送用鍵K dをレシーバ51のSAM62に送信する。ステップS110において、レシーバ51のSAM62は、受信した配送用鍵K dを一時鍵K t e m pで復号し、記憶モジュール73に記憶させる。

【0127】

ステップS111において、EMDサービスセンタ1のユーザ管理部18は、一時鍵Ktempで暗号化した登録リストをレシーバ51のSAM62に送信する。ステップS112において、レシーバ51のSAM62は、受信した登録リストを一時鍵Ktempで復号し、記憶モジュール73に記憶させ、処理は終了する。

【0128】

ステップS107において、受信したIDを有するSAM62が、新規登録であると判定された場合、手続は、ステップS114に進み、EMDサービスセンタ1のユーザ管理部18は、新規登録を実行し、登録リストを作成し、ステップS109に進む。

【0129】

ステップS106において、受信したIDを有するSAM62の登録が不可であると判定された場合、ステップS113に進み、EMDサービスセンタ1のユーザ管理部18は、登録拒絶の登録リストを作成し、ステップS111に進む。

【0130】

このように、レシーバ51は、EMDサービスセンタ1に登録される。

【0131】

次に、今まで使用していたレシーバ51の記憶モジュール73に記憶された配送用鍵Kdなどの所定のデータをICカード55に記憶させる処理の詳細を、図39のフローチャートを参照して説明する。ステップS121において、SAM62の相互認証モジュール71は、ICカード55の相互認証モジュール80と相互認証する。この認証処理は、図33乃至図35を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS122において、SAM62の乱数発生ユニット92は、バックアップ鍵Kicとして用いられる乱数を生成する。ステップS123において、SAM62の暗号化ユニット93は、記憶モジュール73に記憶されているSAMのID番号、保存用鍵Ksave、およびHDD52のIDを、バックアップ鍵Kicを用いて暗号化する。ステップS124において、SAM62の暗号化ユニット93は、EMDサービスセンタ1の公開鍵Kpescでバックアップ鍵Kicを暗号化する（SAM62は、EMDサービスセンタ1との間の認証

処理（図35のステップS89）において、EMDサービスセンタ1の公開鍵K p e s cを取得している）。ステップS125において、レシーバ51のSAM62は、ICカードインターフェース64を介して、暗号化されたSAMのID番号、保存用鍵K s a v e、およびHDD52のID並びに暗号化されたバックアップ鍵K i cをICカード55に送信し、記憶モジュール81に記憶させる。

【0132】

以上のように、SAM62の記憶モジュール73に記憶されたSAMのID番号、保存用鍵K s a v e、およびHDD52のIDは、バックアップ鍵K i cを用いて暗号化され、EMDサービスセンタ1の公開鍵K p e s cを用いて暗号化されたバックアップ鍵K i cと共に、ICカード55の記憶モジュール81に記憶される。

【0133】

今まで使用していたレシーバ51の記憶モジュール73に記憶された配送用鍵K dなどの所定のデータをICカード55に記憶させる他の処理の例の詳細を、図40のフローチャートを参照して説明する。ステップS131において、SAM62の相互認証モジュール71は、ICカード55の相互認証モジュール80と相互認証する。ステップS132において、SAM62の暗号化ユニット93は、記憶モジュール73に記憶されているSAMのID番号、保存用鍵K s a v e、およびHDD52のIDを、EMDサービスセンタ1の公開鍵K p e s cを用いて暗号化する。ステップS133において、レシーバ51のSAM62は、ICカードインターフェース64を介して、暗号化されたSAMのID番号、保存用鍵K s a v e、およびHDD52のIDをICカード55に送信し、記憶モジュール81に記憶させる。

【0134】

図40に示す処理により、図39に示した場合より簡単な処理で、EMDサービスセンタ1の公開鍵K p e s cを用いて暗号化されたSAMのID番号、保存用鍵K s a v e、およびHDD52のIDは、ICカード55の記憶モジュール81に記憶される。

【0135】

このように、ICカード55にバックアップされたデータは、図36のステップS102の処理で、新しいレシーバ51に読み込まれる。図41は、図39に示

す処理でバックアップされたデータ読み出す場合の処理を説明するフローチャートである。ステップS141において、新しいレシーバ51のSAM62の相互認証モジュール71は、ICカード55の相互認証モジュール80と相互認証する。この認証処理は、図33乃至図35を参照して説明した場合と同様であるので、ここでは説明を省略する。

【0136】

ステップS142において、SAM62は、ICカードインタフェース64を介して、記憶モジュール81に記憶された、バックアップ鍵K_{ic}で暗号化されている古いレシーバ51の記憶モジュール73のデータ（SAMのID番号、保存用鍵K_{save}、およびHDD52のIDを示すバックアップデータ）、およびEMDサービスセンタ1の公開鍵K_{pe sc}で暗号化されているバックアップ鍵K_{ic}を読み出す。ステップS143において、SAM62の相互認証モジュール71は、通信部61を介して、EMDサービスセンタ1の相互認証部17と相互認証する。この認証処理は、図33乃至図35を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS144において、SAM62は、通信部61を介して、バックアップ鍵K_{ic}で暗号化されている記憶モジュール73のデータ、およびEMDサービスセンタ1の公開鍵K_{pe sc}で暗号化されているバックアップ鍵K_{ic}を、EMDサービスセンタ1のユーザ管理部18に送信する。

【0137】

ステップS145において、EMDサービスセンタ1のユーザ管理部18は、受信したバックアップ鍵K_{ic}を自分自身の秘密鍵K_{se sc}で復号する。ステップS146において、EMDサービスセンタ1のユーザ管理部18は、受信したバックアップデータを、バックアップ鍵K_{ic}で復号する。ステップS147において、EMDサービスセンタ1のユーザ管理部18は、復号したバックアップデータを、相互認証部17から供給された一時鍵K_{temp}で、再度、暗号化する。

ステップS148において、EMDサービスセンタ1のユーザ管理部18は、一時鍵K_{temp}で暗号化されたバックアップデータを、レシーバ51の通信部61に送信する。

【0138】

ステップS149において、レシーバ51の通信部61は、EMDサービスセンタ1のユーザ管理部18から受信したデータを、SAM62に送信し、SAM62は、そのデータを復号した後、記憶モジュール73に記憶させる。ステップS150において、EMDサービスセンタ1のユーザ管理部18は、ICカード55にデータを記憶させた古い装置のSAM62のIDに対応するユーザ登録データベース（図7）のデータを登録不可に設定し、処理を終了する。

【0139】

このように、新しいレシーバ51は、ICカード55のバックアップデータを読み込む。

【0140】

また、図36のステップS102は、図42に示すフローチャートで説明される処理でもよい。ステップS161乃至ステップS163は、図41のステップS141乃至ステップS143とそれぞれ同様であるので、その説明は省略する。ステップS164において、SAM62は、通信部61を介して、EMDサービスセンタ1の公開鍵K_{pub}で暗号化されているバックアップ鍵K_{ic}を、EMDサービスセンタ1のユーザ管理部18に送信する。

【0141】

ステップS165において、EMDサービスセンタ1のユーザ管理部18は、受信したバックアップ鍵K_{ic}を自分自身の秘密鍵K_{sec}で復号する。ステップS166において、EMDサービスセンタ1のユーザ管理部18は、復号したバックアップ鍵K_{ic}を、相互認証部17から供給された一時鍵K_{temp}で、再度、暗号化する。ステップS167において、EMDサービスセンタ1のユーザ管理部18は、一時鍵K_{temp}で暗号化されたバックアップ鍵K_{ic}を、レシーバ51の通信部61に送信し、バックアップ鍵K_{ic}の復号のサービスに対するユーザへの課金の処理をする。

【0142】

ステップS168において、レシーバ51の通信部61は、EMDサービスセンタ1のユーザ管理部18から受信した一時鍵K_{temp}で暗号化されたバックア

ップ鍵K i cを、SAM 6 2に送信し、SAM 6 2は、一時鍵K t e m pで暗号化されたバックアップ鍵K i cを復号する。ステップS 1 6 9において、SAM 6 2は、復号されたバックアップ鍵K i cで、ステップS 1 6 2においてICカード5 5から読み出された古いレシーバ5 1の記憶モジュール7 3のデータ（SAMのID番号、保存用鍵K s a v e、およびHDD 5 2のIDを示すバックアップデータ）を復号し、記憶モジュール7 3に記憶させる。ステップS 1 7 0において、EMDサービスセンタ1のユーザ管理部1 8は、ICカード5 5にデータを記憶させた古い装置のSAM 6 2のIDに対応するユーザ登録データベース（図7）のデータを登録不可に設定し、処理を終了する。

【0143】

図4 2に示した読み込みの処理は、図4 1に示した処理に比較し、レシーバ5 1とEMDサービスセンタ1の送受信されるデータの量が少なくでき、従って、通信時間を短くできる。図4 1のステップS 1 4 8において、図4 2のステップS 1 6 7と同様に、EMDサービスセンタ1は、課金の処理を行ってもよい。

【0144】

図4 0に示す処理でバックアップされたデータ読み出す場合の処理を、図4 3に示すフローチャートを用いて説明する。ステップS 1 8 1において、新しいレシーバ5 1のSAM 6 2の相互認証モジュール7 1は、ICカード5 5の相互認証モジュール8 0と相互認証する。この認証処理は、図3 3乃至図3 5を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS 1 8 2において、SAM 6 2は、ICカードインタフェース6 4を介して、EMDサービスセンタ1の公開鍵K p e s cで暗号化されている古いレシーバ5 1の記憶モジュール7 3のデータ（SAMのID番号、保存用鍵K s a v e、およびHDD 5 2のIDを示すバックアップデータ）を読み出す。

【0145】

ステップS 1 8 3において、SAM 6 2の相互認証モジュール7 1は、通信部6 1を介して、EMDサービスセンタ1の相互認証部1 7と相互認証する。この認証処理は、図3 3乃至図3 5を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS 1 8 4において、SAM 6 2は、通信部6 1を介して

、EMDサービスセンタ1の公開鍵K p e s cで暗号化されている記憶モジュール73のデータを、EMDサービスセンタ1のユーザ管理部18に送信する。

【0146】

ステップS185において、EMDサービスセンタ1のユーザ管理部18は、受信した記憶モジュール73のデータを自分自身の秘密鍵K s e s cで復号する。ステップS186において、EMDサービスセンタ1のユーザ管理部18は、復号したバックアップデータを、相互認証部17から供給された一時鍵K t e m pで、再度、暗号化する。ステップS187において、EMDサービスセンタ1のユーザ管理部18は、一時鍵K t e m pで暗号化されたバックアップデータを、レシーバ51の通信部61に送信する。

【0147】

ステップS188において、レシーバ51の通信部61は、EMDサービスセンタ1のユーザ管理部18から受信したデータを、SAM62に送信し、SAM62は、そのデータを復号した後、記憶モジュール73に記憶させる。ステップS189において、EMDサービスセンタ1のユーザ管理部18は、ICカード55にデータを記憶させた古い装置のSAM62のIDに対応するユーザ登録データベース（図7）のデータを登録不可に設定する。

【0148】

このように、図40に示す処理を用いたバックアップの場合、図43に示す処理により、新しいレシーバ51は、ICカード55のバックアップデータを読み込む。

【0149】

レシーバ51は、自分自身を登録する場合（図30のステップS12に対応する処理を実行する場合）、図36のフローチャートに示す処理を実行するが、レシーバ51に従属するレコーダ53をEMDサービスセンタ1に登録する場合、図44のフローチャートに示す処理を実行する。ステップS201において、レシーバ51のSAM62は、記憶モジュール73に記憶された登録リストに、レコーダ53のIDを書き込む。ステップS202において、レシーバ51の相互認証モジュール71は、EMDサービスセンタ1の相互認証部17と相互認証する。この

認証処理は、図 3 3 乃至図 3 5 を参照して説明した場合と同様であるので、ここでは説明を省略する。

【0150】

ステップ S 2 0 3 において、EMDサービスセンタ 1 のユーザ管理部 1 8 は、レシーバ 5 1 の ID (図 3 7 に示す SAM 6 2 の証明書に含まれる SAM 6 2 の ID) を基に、ユーザ登録データベースを検索し、レシーバ 5 1 が登録不可であるか否かを判定し、レシーバ 5 1 が登録不可ではないと判定された場合、ステップ S 2 0 4 に進み、レシーバ 5 1 の SAM 6 2 は、EMDサービスセンタ 1 のユーザ管理部 1 8 に、記憶モジュール 7 3 に記憶している配送用鍵 K d のバージョン、課金情報 (後述の図 5 1 に示すフローチャートのステップ S 3 5 7 の処理で記憶される)、および登録リスト、並びに HDD 5 2 に記録された取扱方針を一時鍵 K d で暗号化し、通信部 6 1 を介して、EMDサービスセンタ 1 のユーザ管理部 1 8 に、記憶モジュール 7 3 に記憶している配送用鍵 K d のバージョン、課金情報、および登録リスト、並びに HDD 5 2 に記録された取扱方針を送信する。ステップ S 2 0 5 において、EMDサービスセンタ 1 のユーザ管理部 1 8 は、受信したデータを復号した後、課金情報を処理し、図 3 8 を参照して説明した、レシーバ 5 1 から受信した登録リストのレコーダ 5 3 に関する登録拒絶フラグ、およびステータスフラグなどのデータの部分を更新し、レシーバ 5 1 に対応するデータに応じた署名を付する。

【0151】

ステップ S 2 0 6 において、EMDサービスセンタ 1 のユーザ管理部 1 8 は、レシーバ 5 1 が有する配送用鍵 K d のバージョンが最新か否かを判定し、レシーバ 5 1 が有する配送用鍵 K d のバージョンが最新であると判定された場合、ステップ S 2 0 7 に進み、一時鍵 K d で暗号化した、更新した登録リスト、および課金情報受信メッセージを、レシーバ 5 1 に送信し、レシーバ 5 1 は、更新した登録リスト、および課金情報受信メッセージを受信し、復号した後、記憶する。ステップ S 2 0 8 において、レシーバ 5 1 は、記憶モジュール 7 3 に記憶された課金情報を消去し、登録リストを、EMDサービスセンタ 1 のユーザ管理部 1 8 からステップ S 2 0 7 において受信したものに更新し、ステップ S 2 1 1 に進む。

【0152】

ステップS206において、レシーバ51が有する配送用鍵Kdのバージョンが最新のものではないと判定された場合、ステップS209に進み、EMDサービスセンタ1のユーザ管理部18は、一時鍵Kdで暗号化した、最新バージョンの配送用鍵Kd、更新した登録リスト、および課金情報受信メッセージを、レシーバ51に送信し、レシーバ51は、最新バージョンの配送用鍵Kd、更新した登録リスト、および課金情報受信メッセージを受信し、復号した後、記憶する。ステップS210において、レシーバ51は、記憶モジュール73に記憶された課金情報を消去し、登録リストを、EMDサービスセンタ1のユーザ管理部18からステップS209において受信したものに更新し、配送用鍵Kdを最新バージョンのものに更新し、ステップS211に進む。

【0153】

ステップS211において、レシーバ51のSAM62は、更新した登録リストを参照し、レコーダ53が登録不可か否かを判定し、レコーダ53が登録不可でないと判定された場合、ステップS212に進み、レシーバ51とレコーダ53は相互認証し、一時鍵Ktempを共有する。この認証処理は、図33乃至図35を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS213において、レコーダ53に、一時鍵Kdで暗号化した、登録完了メッセージ、および配送用鍵Kdを送信し、レコーダ53は、登録完了メッセージ、および配送用鍵Kdを受信し、復号する。ステップS214において、レコーダ53は、配送用鍵Kdを更新し、処理は終了する。

【0154】

ステップS203において、レシーバ51が登録不可であると判定された場合、および、ステップS211において、レコーダ53が登録不可であると判定された場合、処理は終了する。

【0155】

以上のように、レシーバ51に従属するレコーダ53は、レシーバ51を介して、EMDサービスセンタ1に登録される。

【0156】

図45は、図30のステップS13において、EMDサービスセンタ1がレシーバ51に送信した配送用鍵Kdを、レシーバ51が受け取る処理の詳細を説明するフローチャートである。ステップS221において、レシーバ51の相互認証モジュール71は、EMDサービスセンタ1の相互認証部17と相互認証する。この認証処理は、図33乃至図35を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS222において、レシーバ51のSAM62は、通信部61を介して、EMDサービスセンタ1のユーザ管理部18に証明書を送信し、EMDサービスセンタ1のユーザ管理部18は、証明書を受信する。ステップS223乃至ステップS230は、図44のステップS203乃至ステップS210と同様の処理であるのでその説明は省略する。

【0157】

このように、レシーバ51は、EMDサービスセンタ1のユーザ管理部18から配送用鍵Kdを受け取り、レシーバ51の課金情報をEMDサービスセンタ1のユーザ管理部18に送信する。

【0158】

次に、レシーバ51に付属するレコーダ53の配送用鍵Kdの受け取り処理（図38に示すステータスフラグが、レコーダ53の配送用鍵Kdの受け取りを許可する値を有する場合）を、図46に示すフローチャートを用いて説明する。ステップS241において、レシーバ51の相互認証モジュール71およびレコーダ53の図示せぬ相互認証モジュールは、相互認証する。この認証処理は、図33乃至図35を参照して説明した場合と同様であるので、ここでは説明を省略する。

【0159】

ステップS242において、レシーバ51は、レシーバ51の記憶モジュール73に記憶する登録リストにレコーダ53のデータが載っているか否かを判定し、レシーバ51の記憶モジュール73に記憶する登録リストにレコーダ53のデータが載っていると判定された場合、ステップS243に進み、レシーバ51の記憶モジュール73に記憶する登録リストを基に、レコーダ53が登録不可であ

るか否かを判定する。ステップS243において、レコーダ53が登録不可ではないと判定された場合、ステップS244に進み、レコーダ53のSAM66は、レシーバ51のSAM62に、内蔵する記憶モジュールに記憶している配送用鍵Kd（後述する図46のステップS255でレシーバ51から受け取っている）のバージョンおよび課金情報（後述する図51に対応する処理のステップS357に相当する処理で記憶している）を一時鍵Ktempで暗号化して、送信し、レシーバ51のSAM62は、配送用鍵Kdのバージョンおよび課金情報を受信し、復号する。

【0160】

ステップS245において、レシーバ51の相互認証モジュール71は、通信部61を介して、EMDサービスセンタ1の相互認証部17と、相互認証する。この認証処理は、図33乃至図35を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS246において、EMDサービスセンタ1のユーザ管理部18は、レシーバ51のIDを基に、ユーザ登録データベースを検索し、レシーバ51が登録不可であるか否かを判定し、レシーバ51が登録不可ではないと判定された場合、ステップS247に進み、レシーバ51のSAM62は、通信部61を介して、EMDサービスセンタ1のユーザ管理部18に、一時鍵Kdで暗号化した、記憶モジュール73に記憶している配送用鍵Kdのバージョン、課金情報、および登録リスト、HDD52に記録している取扱方針、並びにレコーダ53の課金情報を送信する。ステップS248において、EMDサービスセンタ1のユーザ管理部18は、受信したデータを復号した後、課金情報を処理し、図38で説明した、レシーバ51から受信した登録リストのレコーダ53に関する登録拒絶フラグ、ステータスフラグなどのデータの部分を更新し、レシーバ51に対応するデータに応じた署名を付する。

【0161】

ステップS249乃至ステップS254の処理は、図44に示すステップS206乃至ステップS211とそれぞれ同様であるので、その説明は省略する。

【0162】

ステップS254において、レシーバ51のSAM62は、更新した登録リスト

を参照し、レコーダ53が登録不可か否かを判定し、レコーダ53が登録不可でないと判定された場合、ステップS255に進み、レコーダ53に、一時鍵Kdで暗号化した、課金情報受信メッセージ、および配送用鍵Kdを送信し、レコーダ53は、課金情報受信メッセージ、および配送用鍵Kdを受信し、復号する。ステップS256において、レコーダ53のSAM66は、内蔵する記憶モジュールに記憶している、課金情報を消去し、配送用鍵Kdを最新のバージョンに更新する。

【0163】

ステップS242において、レシーバ51の記憶モジュール73に記憶する登録リストにレコーダ53のデータが載っていないと判定された場合、ステップS257に進み、図44に示したレコーダ53の登録処理を実行し、ステップS244に進む。

【0164】

ステップS243において、レコーダ53が登録不可であると判定された場合、ステップS246において、レシーバ51が登録不可であると判定された場合、および、ステップS254において、レコーダ53が登録不可であると判定された場合、処理は終了する。

【0165】

以上のように、レシーバ51に従属するレコーダ53は、レシーバ51を介して、配送用鍵Kdを受け取る。

【0166】

次に、図30のステップS14に対応する、コンテンツプロバイダ2がサービスプロバイダ3にコンテンツプロバイダセキュアコンテナを送信する処理を、図47のフローチャートを用いて説明する。ステップS271において、コンテンツプロバイダ2のウォータマーク付加部32は、コンテンツサーバ31から読み出したコンテンツに、コンテンツプロバイダ2を示す所定のウォータマークを挿入し、圧縮部33に供給する。ステップS272において、コンテンツプロバイダ2の圧縮部33は、ウォータマークが挿入されたコンテンツをATRAC2等の所定の方式で圧縮し、暗号化部34に供給する。ステップS273において、乱数発

生部35は、コンテンツ鍵K_{co}として用いる乱数を発生させ、暗号化部34に供給する。ステップS274において、コンテンツプロバイダ2の暗号化部34は、DESなどの所定の方式で、コンテンツ鍵K_{co}を使用して、ウォーターマークが挿入され、圧縮されたコンテンツを暗号化する。

【0167】

ステップS275において、暗号化部36は、DESなどの所定の方式で、図30のステップS11の処理により、EMDサービスセンタ1から供給されている配送用鍵K_dでコンテンツ鍵K_{co}を暗号化する。ステップS276において、コンテンツプロバイダ2のセキュアコンテナ作成部38は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵K_{co}、およびポリシー記憶部37から供給された取扱方針にハッシュ関数を適用してハッシュ値を算出し、自分自身の秘密鍵K_{scp}で暗号化し、図13に示すような署名を作成する。ステップS277において、コンテンツプロバイダ2のセキュアコンテナ作成部38は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵K_{co}、ポリシー記憶部37から供給される取扱方針、およびステップS276で生成した署名を含んだ、図13に示すようなコンテンツプロバイダセキュアコンテナを作成する。

【0168】

ステップS278において、コンテンツプロバイダ2の相互認証部39は、サービスプロバイダ3の相互認証部45と相互認証する。この認証処理は、図33乃至図35を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS279において、コンテンツプロバイダ2のセキュアコンテナ作成部38は、サービスプロバイダ3に、コンテンツプロバイダセキュアコンテナに、予め認証局から発行してもらった証明書を付して送信し、処理を終了する。

【0169】

以上のように、コンテンツプロバイダ2は、サービスプロバイダ3に、コンテンツプロバイダセキュアコンテナを送信する。

【0170】

コンテンツ鍵K_{co}と共に取扱方針を配送用鍵K_dで暗号化する例の場合の、コンテンツプロバイダ2がサービスプロバイダ3にコンテンツプロバイダセキュア

アコンテナを送信する他の処理の詳細を、図48のフローチャートを用いて説明する。ステップS291乃至ステップS294の処理は、図47のステップS271乃至ステップS274の処理とそれぞれ同様であり、その説明は省略する。ステップS295において、コンテンツプロバイダ2の暗号化部36は、図31のステップS21の処理により、EMDサービスセンタ1から供給されている配送用鍵K_dを用いて、DESなどの所定の方式で、コンテンツ鍵K_{co}およびポリシー記憶部37から供給される取扱方針を暗号化する。

【0171】

ステップS296において、コンテンツプロバイダ2のセキュアコンテナ作成部38は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵K_{co}、および暗号化された取扱方針にハッシュ関数を適用しハッシュ値を算出し、自分自身の秘密鍵K_{scp}で暗号化し、図25に示すような署名を作成する。ステップS297において、コンテンツプロバイダ2のセキュアコンテナ作成部38は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵K_{co}、暗号化された取扱方針、および署名を含んだ、図25に示すようなコンテンツプロバイダセキュアコンテナを作成する。ステップS298およびステップS299の処理は、図47のステップS278およびステップS279の処理とそれぞれ同様であり、その説明は省略する。

【0172】

このように、コンテンツプロバイダ2は、サービスプロバイダ3に、暗号化された取扱方針を含むコンテンツプロバイダセキュアコンテナを送信する。

【0173】

次に、図30のステップS15に対応する、サービスプロバイダ3がレシーバ51にサービスプロバイダセキュアコンテナを送信する処理の詳細を図49のフローチャートを用いて説明する。ステップS311において、サービスプロバイダ3の値付け部42は、コンテンツプロバイダ2のセキュアコンテナ作成部38から送信されたコンテンツプロバイダセキュアコンテナに付された証明書に含まれる署名を確認し、証明書の改竄がなければ、コンテンツプロバイダ2の公開鍵K_{pcp}を取り出す。証明書の署名の確認は、図3.5のステップS83における

処理と同様であるので、その説明は省略する。

【0174】

ステップS312において、サービスプロバイダ3の値付け部42は、コンテンツプロバイダ2のセキュアコンテンツ作成部38から送信されたコンテンツプロバイダセキュアコンテンツの署名をコンテンツプロバイダ2の公開鍵K_{pcp}で復号し、得られたハッシュ値が、暗号化されたコンテンツ、暗号化されたコンテンツ鍵K_{co}、および取扱方針にハッシュ関数を適用し得られたハッシュ値と一致することを確認し、コンテンツプロバイダセキュアコンテンツの改竄がないことを確認する。改竄が発見された場合は、処理を終了する。

【0175】

コンテンツプロバイダセキュアコンテンツに改竄がない場合、ステップS313において、サービスプロバイダ3の値付け部42は、コンテンツプロバイダセキュアコンテンツから取扱方針を取り出す。ステップS314において、サービスプロバイダ3の値付け部42は、取扱方針を基に、図17で説明した価格情報を作成する。ステップS315において、サービスプロバイダ3のセキュアコンテンツ作成部44は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵K_{co}、取扱方針、価格情報、並びに暗号化されたコンテンツ、暗号化されたコンテンツ鍵K_{co}、取扱方針、および価格情報にハッシュ関数を適用して得られたハッシュ値を、自分自身の秘密鍵K_{ssp}で暗号化し、得られた値を署名として図15に示すようなサービスプロバイダセキュアコンテンツを作成する。

【0176】

ステップS316において、サービスプロバイダ3の相互認証部45は、レシーバ51の相互認証モジュール71と相互認証する。この認証処理は、図33乃至図35を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS317において、サービスプロバイダ3のセキュアコンテンツ作成部44は、レシーバ51の通信部61に、証明書を付したサービスプロバイダセキュアコンテンツを送信し、処理を終了する。

【0177】

このように、サービスプロバイダ3は、レシーバ51にサービスプロバイダセ

キュアコンテナを送信する。

【0178】

コンテンツプロバイダ2において、取扱方針が配送用鍵Kdで暗号化され、かつ、サービスプロバイダ3が取扱制御情報を作成する例の場合の、サービスプロバイダ3がレシーバ51にサービスプロバイダセキュアコンテナを送信する処理の詳細を、図50のフローチャートを用いて説明する。ステップS331およびステップS332の処理は、図49のステップS311およびステップS312の処理とそれぞれ同様であるので、その説明は省略する。ステップS333において、サービスプロバイダ3の値付け部42は、コンテンツプロバイダセキュアコンテナに含まれる暗号化された取扱方針を復号する。ステップS334において、サービスプロバイダ3の値付け部42は、取扱方針を基に、図23で説明した取扱制御情報を作成する。ステップS335乃至ステップS338の処理は、図49のステップS314およびステップS317の処理とそれぞれ同様であるので、その説明は省略する。

【0179】

このように、サービスプロバイダ3は、レシーバ51に暗号化された取扱方針を含むサービスプロバイダセキュアコンテナを送信する。

【0180】

図30のステップS16に対応する、適正なサービスプロバイダセキュアコンテナを受信した後の、レシーバ51の課金処理の詳細を、図51のフローチャートを用いて説明する。ステップS351において、レシーバ51の復号/暗号化モジュール74は、配送用鍵Kdでコンテンツ鍵Kcoを復号できるか否かを判定し、配送用鍵Kdでコンテンツ鍵Kcoを復号できないと判定された場合、ステップS352で、レシーバ51は、図45で説明した配送用鍵Kdの受け取り処理を実行し、ステップS353に進む。ステップS351において、配送用鍵Kdでコンテンツ鍵Kcoを復号できると判定された場合、手続は、ステップS352をスキップし、ステップS353に進む。ステップS353において、レシーバ51の復号ユニット91は、図30のステップS13の処理により、記憶モジュール73に記憶されている配送用鍵Kdで、コンテンツ鍵Kcoを復号す

る。

【0181】

ステップS354において、レシーバ51の課金処理モジュール72は、サービスプロバイダセキュアコンテナに含まれる取扱方針および価格情報を取り出し、図19および図20で説明した課金情報および使用許諾条件情報を生成する。ステップS355において、レシーバ51の課金処理モジュール72は、記憶モジュール73に記憶している課金情報およびステップS354で算出された課金情報から、現在の課金が課金の上限以上であるか否かを判定し、現在の課金が課金の上限以上であると判定された場合、ステップS356に進み、レシーバ51は図45で説明した配送用鍵Kdの受け取り処理を実行し、新たな配送用鍵Kdを受け取り、ステップS357に進む。ステップS355において、現在の課金が課金の上限未満であると判定された場合、ステップS356はスキップされ、ステップS357に進む。

【0182】

ステップS357において、レシーバ51の課金処理モジュール72は、記憶モジュール73に課金情報を記憶させる。ステップS358において、レシーバ51の課金処理モジュール72は、ステップS354にて生成した使用許諾条件情報をHDD52に記録する。ステップS359において、レシーバ51のSAM62は、HDD52にサービスプロバイダセキュアコンテナから取り出した取扱方針を記録させる。

【0183】

ステップS360において、レシーバ51の復号／暗号化モジュール74は、使用許諾条件情報にハッシュ関数を適用しハッシュ値を算出する。ステップS361において、レシーバ51の記憶モジュール73は、使用許諾条件情報のハッシュ値を記憶する。記憶モジュール73に保存用鍵Ksaveが記憶されていない場合、ステップS362において、レシーバ51の乱数発生ユニット92は、保存用鍵Ksaveである乱数を発生し、ステップS363に進む。記憶モジュール73に保存用鍵Ksaveが記憶されている場合、ステップS362はスキップされ、ステップS363に進む。

【0184】

ステップS363において、レシーバ51の暗号化ユニット93は、コンテンツ鍵Kcoを保存用鍵Ksaveで暗号化する。ステップS364において、レシーバ51のSAM62は、暗号化されたコンテンツ鍵KcoをHDD52に記憶させる。記憶モジュール73に保存用鍵Ksaveが記憶されていない場合、ステップS365において、レシーバ51の復号/暗号化モジュール74は、保存用鍵Ksaveを記憶モジュール73に記憶させ、処理は終了する。記憶モジュール73に保存用鍵Ksaveが記憶されている場合、ステップS365はスキップされ、処理は終了する。

【0185】

以上のように、レシーバ51は、課金情報を記憶モジュール73に記憶すると共に、コンテンツ鍵Kcoを配送用鍵Kdで復号し、再度、コンテンツ鍵Kcoを保存用鍵Ksaveで暗号化し、HDD52に記録させる。保存用鍵Ksaveは、記憶モジュール73に記憶されている。

【0186】

レコーダ53も、同様の処理で、課金情報をSAM66内の記憶モジュールに記憶すると共に、コンテンツ鍵Kcoを配送用鍵Kdで復号し、再度、コンテンツ鍵Kcoを保存用鍵Ksaveで暗号化し、HDD52に記録させる。保存用鍵Ksaveは、SAM66内の記憶モジュールに記憶されている。

【0187】

図30のステップS17に対応するレシーバ51がコンテンツを再生する処理の詳細を、図52のフローチャートを用いて説明する。ステップS381において、レシーバ51の復号/暗号化モジュール74は、HDD52から、図51のステップS358で記憶した使用許諾条件情報およびステップS364で記憶した暗号化されたコンテンツ鍵Kcoを読み出す。ステップS382において、レシーバ51の復号/暗号化モジュール74は、使用許諾条件情報にハッシュ関数を適用しハッシュ値を算出する。

【0188】

ステップS383において、レシーバ51の復号/暗号化モジュール74は、

ステップS382において算出されたハッシュ値が、図51のステップS360で記憶モジュール73に記憶されたハッシュ値と一致するか否かを判定し、ステップS382において算出されたハッシュ値が、記憶モジュール73に記憶されたハッシュ値と一致すると判定された場合、ステップS384に進み、使用回数の値などの使用許諾条件情報に含まれる所定の情報を更新する。ステップS385において、レシーバ51の復号／暗号化モジュール74は、更新した使用許諾条件情報にハッシュ関数を適用しハッシュ値を算出する。ステップS386において、レシーバ51の記憶モジュール73は、ステップS385で算出した使用許諾条件情報のハッシュ値を記憶する。ステップS387において、レシーバ51の復号／暗号化モジュール74は、HDD52に更新した使用許諾条件情報を記録させる。

【0189】

ステップS388において、SAM62の相互認証モジュール71と伸張部63の相互認証モジュール75は、相互認証し、SAM62および伸張部63は、一時鍵Ktempを記憶する。この認証処理は、図33乃至図35を参照して説明した場合と同様であるので、ここでは説明を省略する。相互認証に用いられる乱数R1、R2、またはR3が、一時鍵Ktempとして用いられる。ステップS389において、復号／暗号化モジュール74の復号ユニット91は、図51のステップS364にてHDD52に記録されたコンテンツ鍵Kcoを、記憶モジュール73に記憶された保存用鍵Ksaveで復号する。ステップS390において、復号／暗号化モジュール74の暗号化ユニット93は、復号されたコンテンツ鍵Kcoを一時鍵Ktempで暗号化する。ステップS391において、SAM62は、一時鍵Ktempで暗号化されたコンテンツ鍵Kcoを伸張部63に送信する。

【0190】

ステップS392において、伸張部63の復号モジュール76は、コンテンツ鍵Kcoを一時鍵Ktempで復号する。ステップS393において、SAM62は、HDD52に記録されたコンテンツを読み出し、伸張部63に送信する。ステップS394において、伸張部63の復号モジュール77は、コンテンツをコン

テンツ鍵K c oで復号する。ステップS 3 9 5において、伸張部6 3の伸張モジュール7 8は、復号されたコンテンツをATRAC2などの所定の方式で伸張する。ステップS 3 9 6において、伸張部6 3のウォータマーク付加モジュール7 9は、伸張されたコンテンツにレシーバ5 1を特定する所定のウォータマークを挿入する。ステップS 3 9 7において、レシーバ5 1は、図示せぬスピーカなどに再生されたコンテンツを出力し、処理を終了する。

【0191】

ステップS 3 8 3において、ステップS 3 8 2において算出されたハッシュ値が、記憶モジュール7 3に記憶されたハッシュ値と一致しないと判定された場合、ステップS 3 9 8において、SAM 6 2は、図示せぬ表示装置にエラーメッセージを表示させる等の所定のエラー処理を実行し、処理は終了する。

【0192】

このように、レシーバ5 1は、コンテンツを再生する。

【0193】

図5 3は、図1 1の構成を有するユーザホームネットワーク5において、レシーバ5 1がデコーダ5 6にコンテンツを再生させる処理を説明するフローチャートである。ステップS 4 1 1乃至ステップS 4 1 7の処理は、図5 2のステップS 3 8 1乃至ステップS 3 8 7の処理とそれぞれ同様であるので、その説明は省略する。

【0194】

ステップS 4 1 8において、SAM 6 2の相互認証モジュール7 1とデコーダ5 6の相互認証モジュール1 0 1は、相互認証し、一時鍵K t e m pが共有される。この認証処理は、図3 3乃至図3 5を参照して説明した場合と同様であるので、ここでは説明を省略する。相互認証に用いられる乱数R 1、R 2、またはR 3が、一時鍵K t e m pとして用いられる。ステップS 4 1 9において、復号/暗号化モジュール7 4の復号ユニット9 1は、HDD 5 2に記録されたコンテンツ鍵K c oを、記憶モジュール7 3に記憶された保存用鍵K s a v eで復号する。ステップS 4 2 0において、復号/暗号化モジュール7 4の暗号化ユニット9 3は、復号されたコンテンツ鍵K c oを一時鍵K t e m pで暗号化する。ステップS

421において、SAM62は、一時鍵Ktempで暗号化されたコンテンツ鍵Kcoをデコーダ56に送信する。

【0195】

ステップS422において、デコーダ56の復号モジュール102は、コンテンツ鍵Kcoを一時鍵Ktempで復号する。ステップS423において、SAM62は、HDD52に記録されたコンテンツを読み出し、デコーダ56に送信する。ステップS424において、デコーダ56の復号モジュール103は、コンテンツをコンテンツ鍵Kcoで復号する。ステップS425において、デコーダ56の伸張モジュール104は、復号されたコンテンツをATRAC2などの所定の方式で伸張する。ステップS426において、デコーダ56のウォーターマーク付加モジュール105は、伸張されたコンテンツにデコーダ56を特定する所定のウォーターマークを挿入する。ステップS427において、デコーダ56は、図示せぬスピーカなどに再生されたコンテンツを出力し、処理を終了する。

【0196】

ステップS428の処理は、図52のステップS398の処理と同様であるので、その説明は省略する。

【0197】

以上のように、ユーザホームネットワークが図11に示す構成を有する場合、レシーバ51が受信したコンテンツは、デコーダ56で再生される。

【0198】

なお、コンテンツは、音楽データを例に説明したが、音楽データに限らず、動画像データ、静止画像データ、文書データ、またはプログラムデータでもよい。その際、圧縮は、コンテンツの種類に適した方式、例えば、画像であればMPEG(Moving Picture Experts Group)などが利用される。ウォーターマークも、コンテンツの種類に適した形式のウォーターマークが利用される。

【0199】

また、共通鍵暗号は、ブロック暗号であるDESを使用して説明したが、NTT(商標)が提案するFEAL、IDEA(International Data Encryption Algorithm)、または1ビット乃至数ビット単位で暗号化するストリーム暗号などでもよい。

【0200】

さらに、コンテンツおよびコンテンツ鍵K_{co}の暗号化は、共通鍵暗号方式を利用するとして説明したが、公開鍵暗号方式でもよい。

【0201】

なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものとする。

【0202】

また、上記したような処理を行うコンピュータプログラムをユーザに提供する提供媒体としては、磁気ディスク、CD-ROM、固体メモリなどの記録媒体の他、ネットワーク、衛星などの通信媒体を利用することができる。

【0203】

【発明の効果】

請求項1に記載の情報処理装置、請求項3に記載の情報処理方法、および請求項4に記載の提供媒体によれば、装着された外部記憶媒体と相互認証し、所定の鍵で所定の情報を暗号化するようにしたので、不正に対する安全性を保持したまま、必要な情報を外部に記憶できる。

【0204】

請求項5に記載の管理装置、請求項6に記載の管理方法、および請求項7に記載の提供媒体によれば、情報処理装置に装着された外部記憶媒体に記憶されたデータを復号するようにしたので、不正に対する安全性を保持したまま、必要な情報を外部に記憶できる。

【0205】

請求項8に記載の情報利用システムによれば、情報処理装置が、装着された外部記憶媒体と相互認証し、管理装置の公開鍵で所定の情報を暗号化し、管理装置が、外部記憶媒体に記憶されたデータを復号するようにしたので、不正に対する安全性を保持したまま、必要な情報を外部に記憶できる。

【0206】

請求項9に記載の外部記憶媒体によれば、情報処理装置と相互認証するようにしたので、不正な読み取りを防止できる。

【図面の簡単な説明】

【図 1】

EMDのシステムを説明する図である。

【図 2】

EMDサービスセンタ 1 の機能の構成を示すブロック図である。

【図 3】

EMDサービスセンタ 1 の配送用鍵 K d の送信を説明する図である。

【図 4】

EMDサービスセンタ 1 の配送用鍵 K d の送信を説明する図である。

【図 5】

EMDサービスセンタ 1 の配送用鍵 K d の送信を説明する図である。

【図 6】

EMDサービスセンタ 1 の配送用鍵 K d の送信を説明する図である。

【図 7】

ユーザ登録データベースを説明する図である。

【図 8】

コンテンツプロバイダ 2 の機能の構成を示すブロック図である。

【図 9】

サービスプロバイダ 3 の機能の構成を示すブロック図である。

【図 10】

ユーザホームネットワーク 5 の構成を示すブロック図である。

【図 11】

ユーザホームネットワーク 5 の構成を示すブロック図である。

【図 12】

コンテンツおよびコンテンツに付随する情報を説明する図である。

【図 13】

コンテンツプロバイダセキュアコンテナを説明する図である。

【図 14】

コンテンツプロバイダ 2 の証明書を説明する図である。

【図 1 5】

サービスプロバイダセキュアコンテナを説明する図である。

【図 1 6】

サービスプロバイダ 3 の証明書を説明する図である。

【図 1 7】

取扱方針、価格情報、および使用許諾条件情報を示す図である。

【図 1 8】

シングルコピーおよびマルチコピーを説明する図である。

【図 1 9】

取扱方針および価格情報を説明する図である。

【図 2 0】

取扱方針、価格情報、および使用許諾条件情報を説明する図である。

【図 2 1】

コンテンツおよびコンテンツに付随する情報の他の構成を説明する図である。

【図 2 2】

サービスプロバイダセキュアコンテナを説明する図である。

【図 2 3】

取扱方針、取扱制御情報、価格情報、及び使用許諾条件の構成を示す図である。

【図 2 4】

コンテンツおよびコンテンツに付随する情報の他の構成を説明する図である。

【図 2 5】

コンテンツプロバイダセキュアコンテナを説明する図である。

【図 2 6】

サービスプロバイダセキュアコンテナを説明する図である。

【図 2 7】

EMDサービスセンタ 1 の、ユーザホームネットワーク 5 からの課金情報の受信のときの動作を説明する図である。

【図 28】

EMDサービスセンタ 1 の利益分配処理の動作を説明する図である。

【図 29】

EMDサービスセンタ 1 の、コンテンツの利用実績の情報を JASRAC に送信する処理の動作を説明する図である。

【図 30】

コンテンツの配布の処理を説明するフローチャートである。

【図 31】

コンテンツの配布の処理を説明するフローチャートである。

【図 32】

EMDサービスセンタ 1 がコンテンツプロバイダ 2 へ配送用鍵 K d を送信する処理を説明するフローチャートである。

【図 33】

コンテンツプロバイダ 2 と EMD サービスセンタ 1 との相互認証の動作を説明するフローチャートである。

【図 34】

コンテンツプロバイダ 2 と EMD サービスセンタ 1 との相互認証の動作を説明するフローチャートである。

【図 35】

コンテンツプロバイダ 2 と EMD サービスセンタ 1 との相互認証の動作を説明するフローチャートである。

【図 36】

レシーバ 5 1 の EMD サービスセンタ 1 への登録の処理を説明するフローチャートである。

【図 37】

SAM の証明書を説明する図である。

【図 38】

登録リストを説明する図である。

【図39】

ICカード55へのSAM62のデータのバックアップの処理を説明するフローチャートである。

【図40】

ICカード55へのSAM62のデータのバックアップの処理を説明するフローチャートである。

【図41】

新しいレシーバにICカード55のバックアップデータを読み込ませる処理を説明するフローチャートである。

【図42】

新しいレシーバにICカード55のバックアップデータを読み込ませる処理を説明するフローチャートである。

【図43】

新しいレシーバにICカード55のバックアップデータを読み込ませる処理を説明するフローチャートである。

【図44】

レシーバ51が、従属関係のあるレコーダ53をEMDサービスセンタ1に登録する処理を説明するフローチャートである。

【図45】

レシーバ51がEMDサービスセンタ1から配送用鍵Kdを受け取る処理を説明するフローチャートである。

【図46】

レコーダの配送用鍵Kdの受け取り処理を説明するフローチャートである。

【図47】

コンテンツプロバイダ2がサービスプロバイダ3にコンテンツプロバイダセキュリティコンテナを送信する処理を説明するフローチャートである。

【図48】

コンテンツプロバイダ2がサービスプロバイダ3にコンテンツプロバイダセキュリティコンテナを送信する他の処理を説明するフローチャートである。

【図 49】

サービスプロバイダ 3 がレシーバ 51 にサービスプロバイダセキュアコンテンツを送信する処理を説明するフローチャートである。

【図 50】

サービスプロバイダ 3 がレシーバ 51 にサービスプロバイダセキュアコンテンツを送信する処理を説明するフローチャートである。

【図 51】

レシーバ 51 の課金処理を説明するフローチャートである。

【図 52】

レシーバ 51 がコンテンツを再生する処理を説明するフローチャートである。

【図 53】

レシーバ 51 がデコーダ 56 にコンテンツを再生させる処理を説明するフローチャートである。

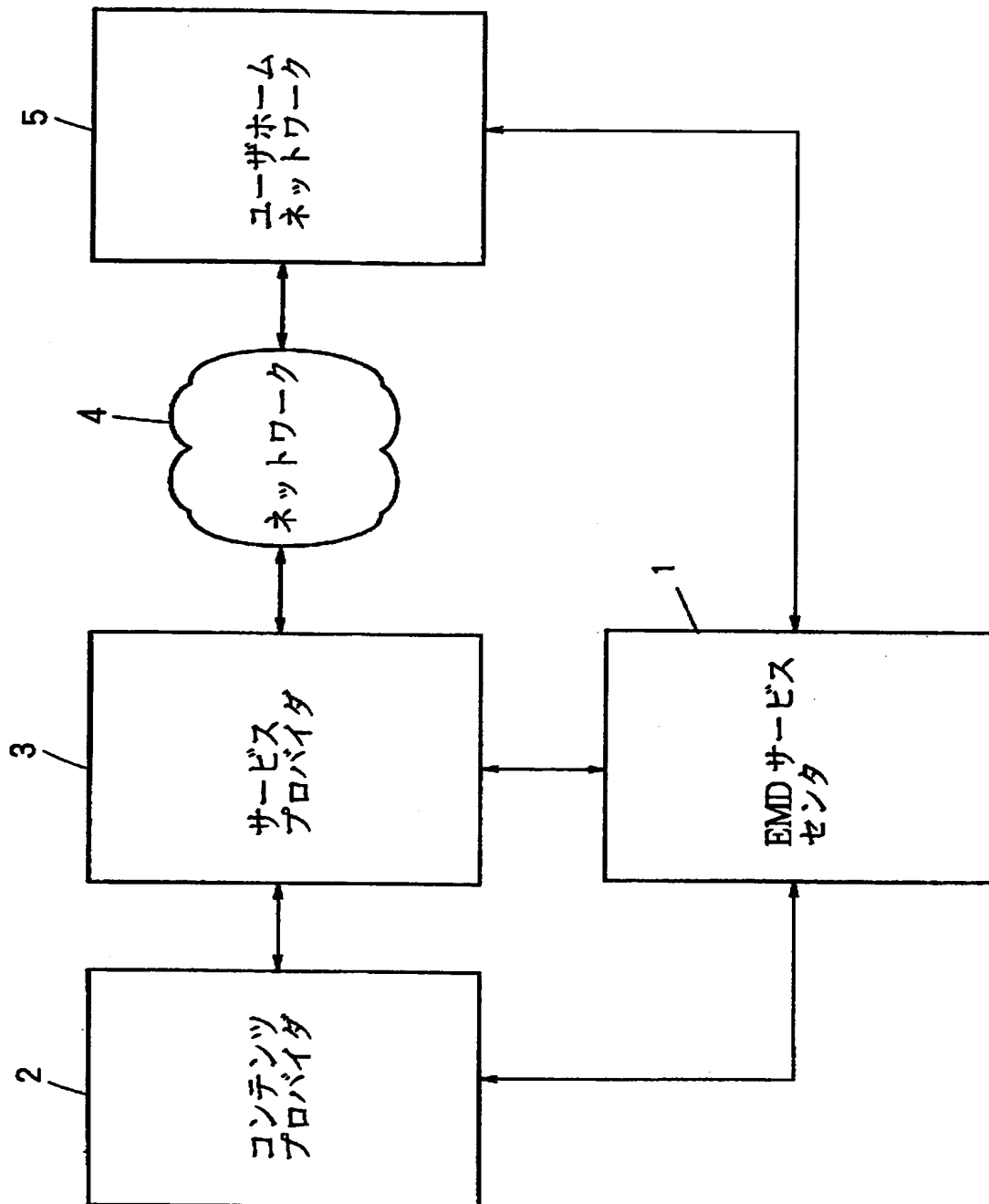
【符号の説明】

1 EMDサービスセンタ, 2 コンテンツプロバイダ, 3 サービスプロバイダ, 5 ユーザホームネットワーク, 16 利益分配部, 18 ユーザ管理部, 42 値付け部, 51 レシーバ, 56 デコーダ, 61 通信部, 62 SAM, 63 伸張部, 71 相互認証モジュール, 72 課金処理モジュール, 73 記憶モジュール, 74 復号/暗号化モジュール, 75 相互認証モジュール, 76 復号モジュール, 77 復号モジュール, 81 相互認証モジュール, 91 復号ユニット, 92 暗号化ユニット, 93 暗号化ユニット, 101 相互認証モジュール, 102 復号モジュール, 103 復号モジュール

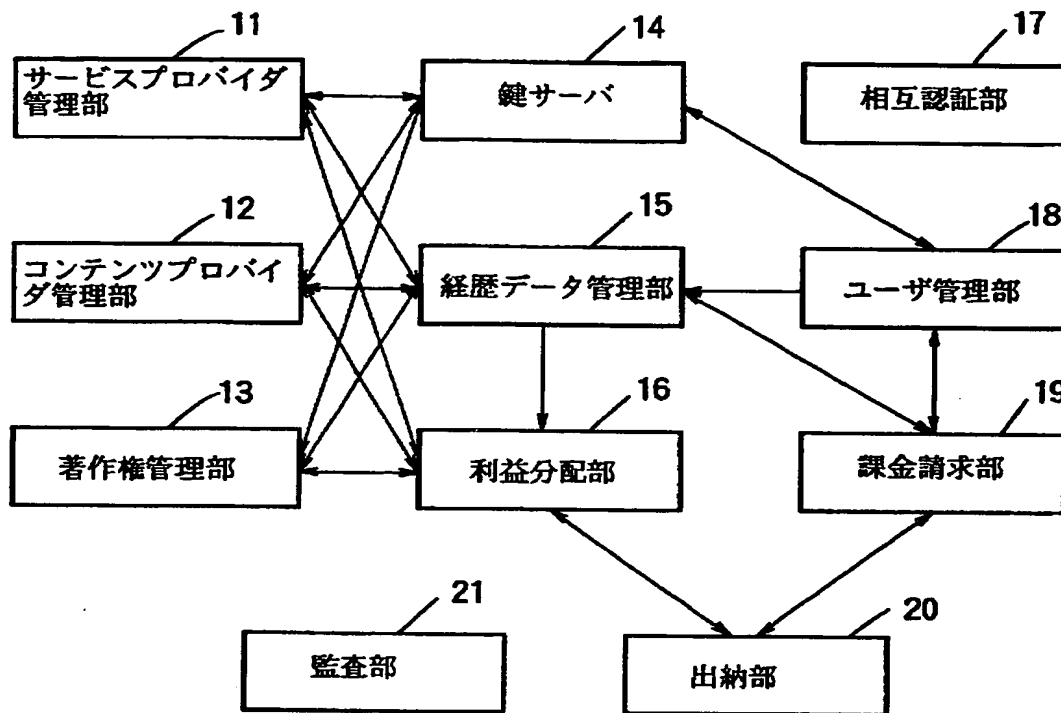
【書類名】

図面

【図 1】

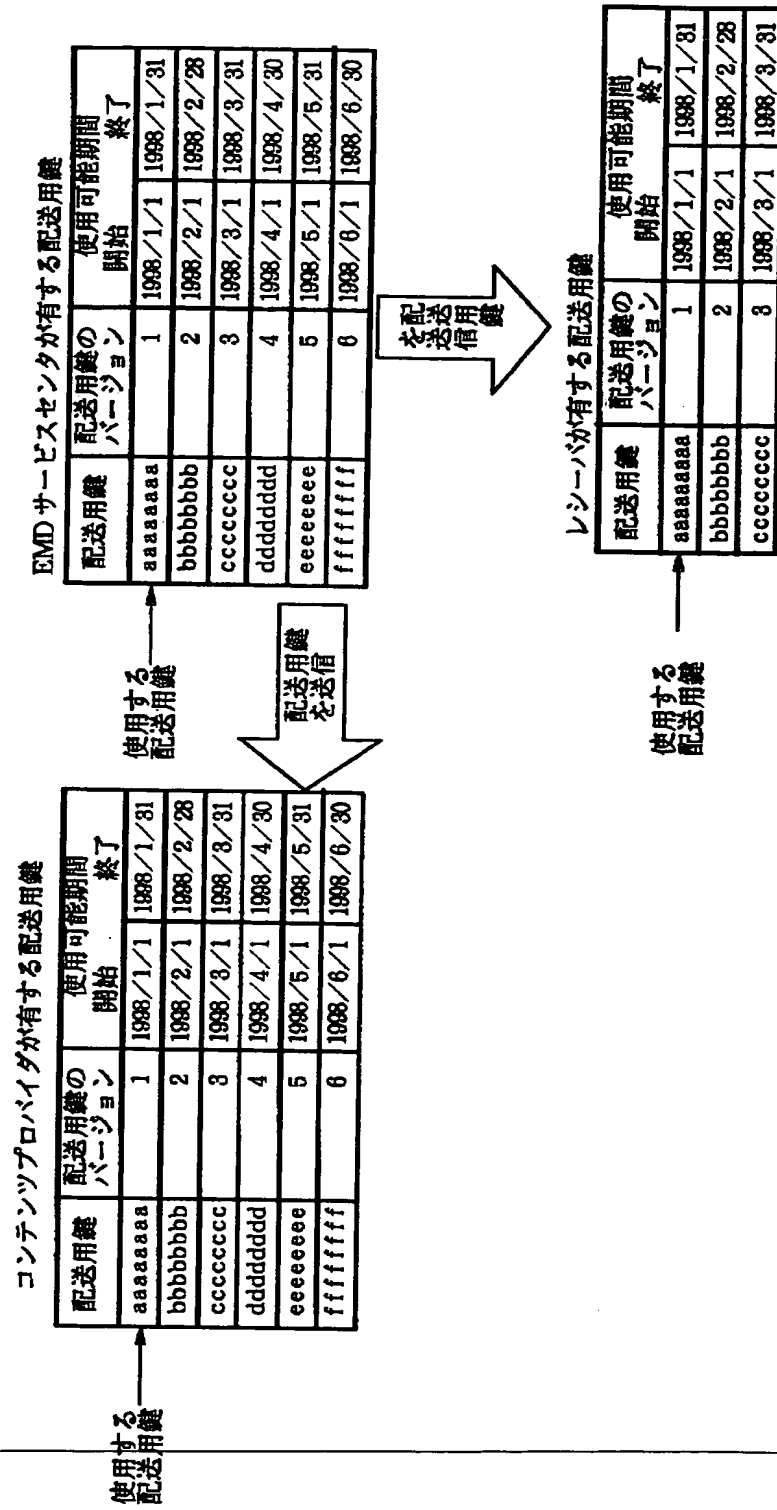


【図 2】

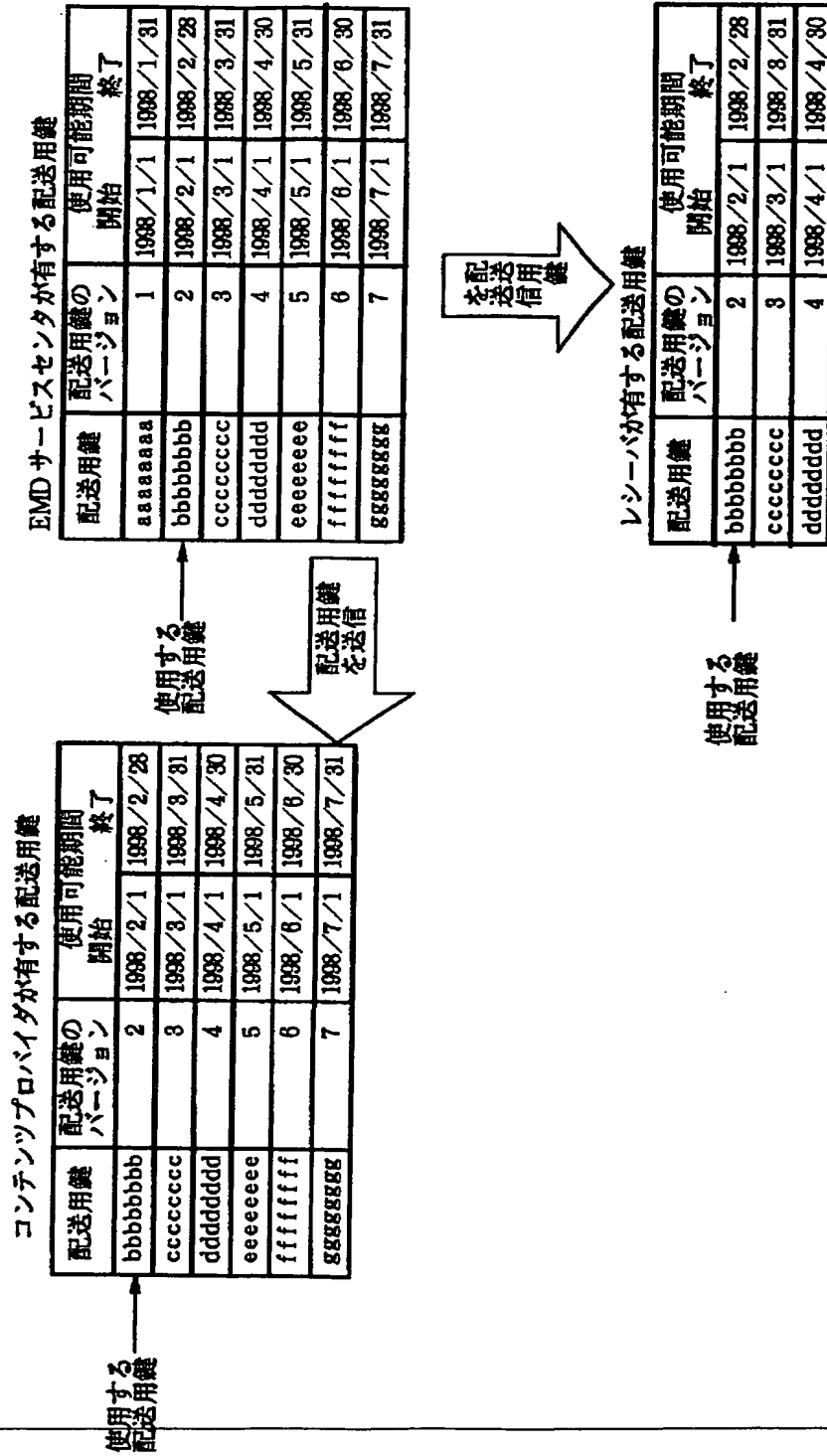


EMD サービスセンタ 1

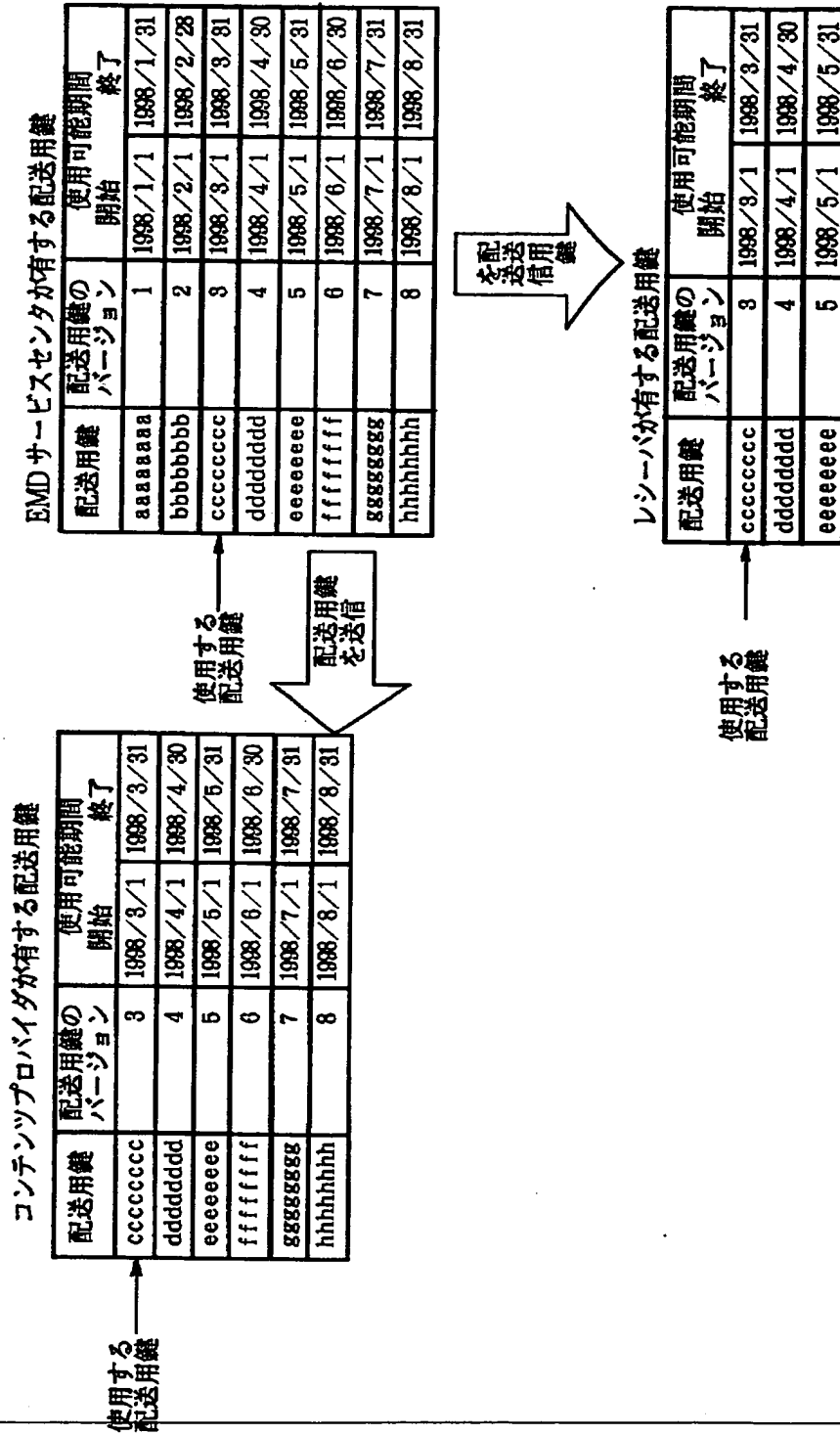
【図 3】



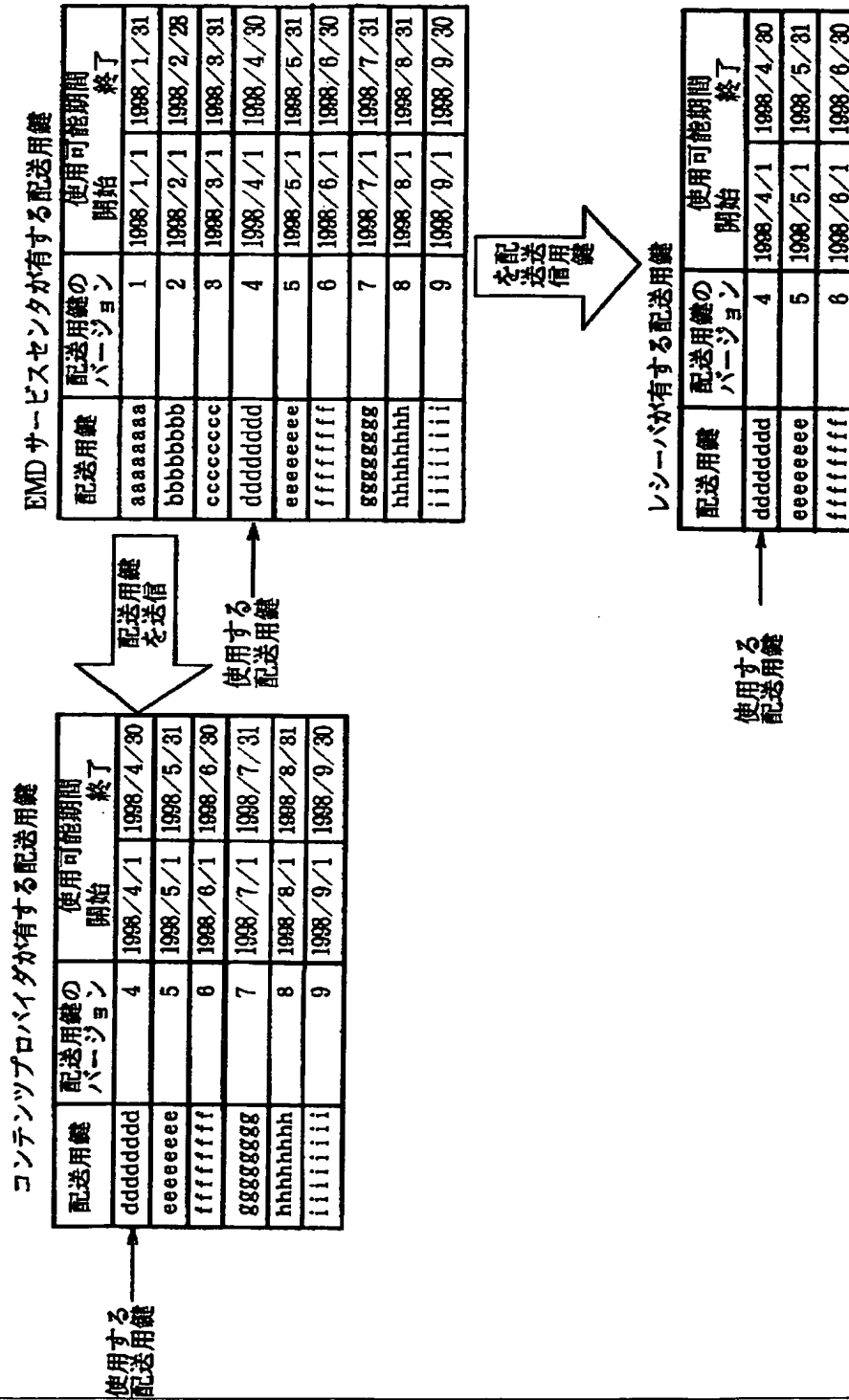
【図 4】



【図 5】



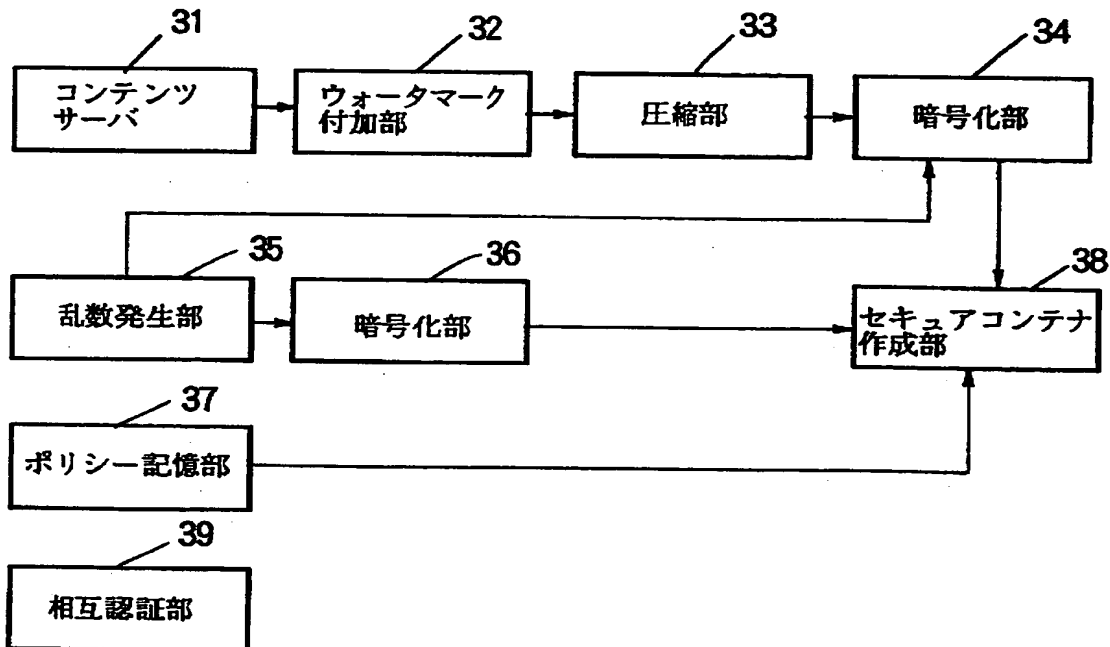
【図 6】



【図 7】

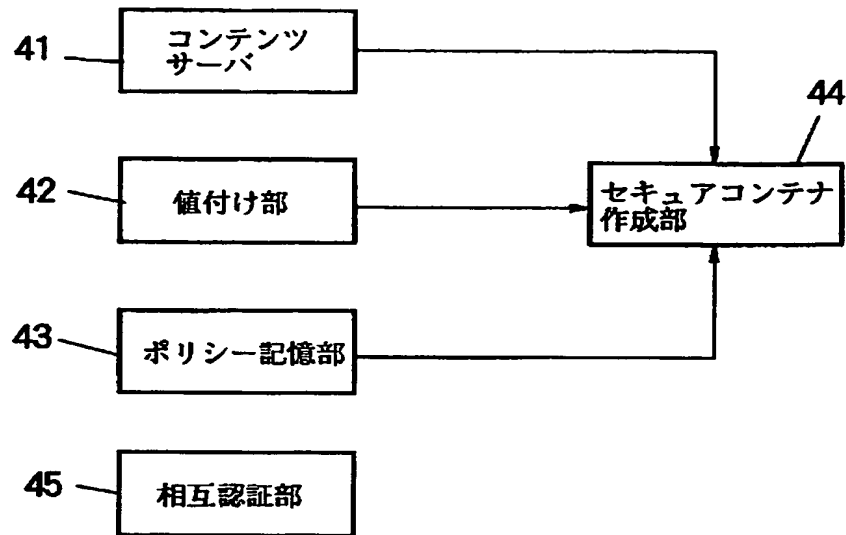
ID	決済処理	登録	EMD サービスセンタとの接続
0000000000000001h	可	可	可
0000000000000002h	可	可	不可
0000000000000003h	可	不可	可
0000000000000004h	可	不可	不可
0000000000000005h	不可	可	可
0000000000000006h	不可	可	不可
0000000000000007h	不可	不可	可
0000000000000008h	不可	不可	不可
0000000000000009h	可	可	可
...			
FFFFFFFFFFFFFFFFh	可	不可	不可
FFFFFFFFFFFFFFFFh	不可	可	可

【図 8】



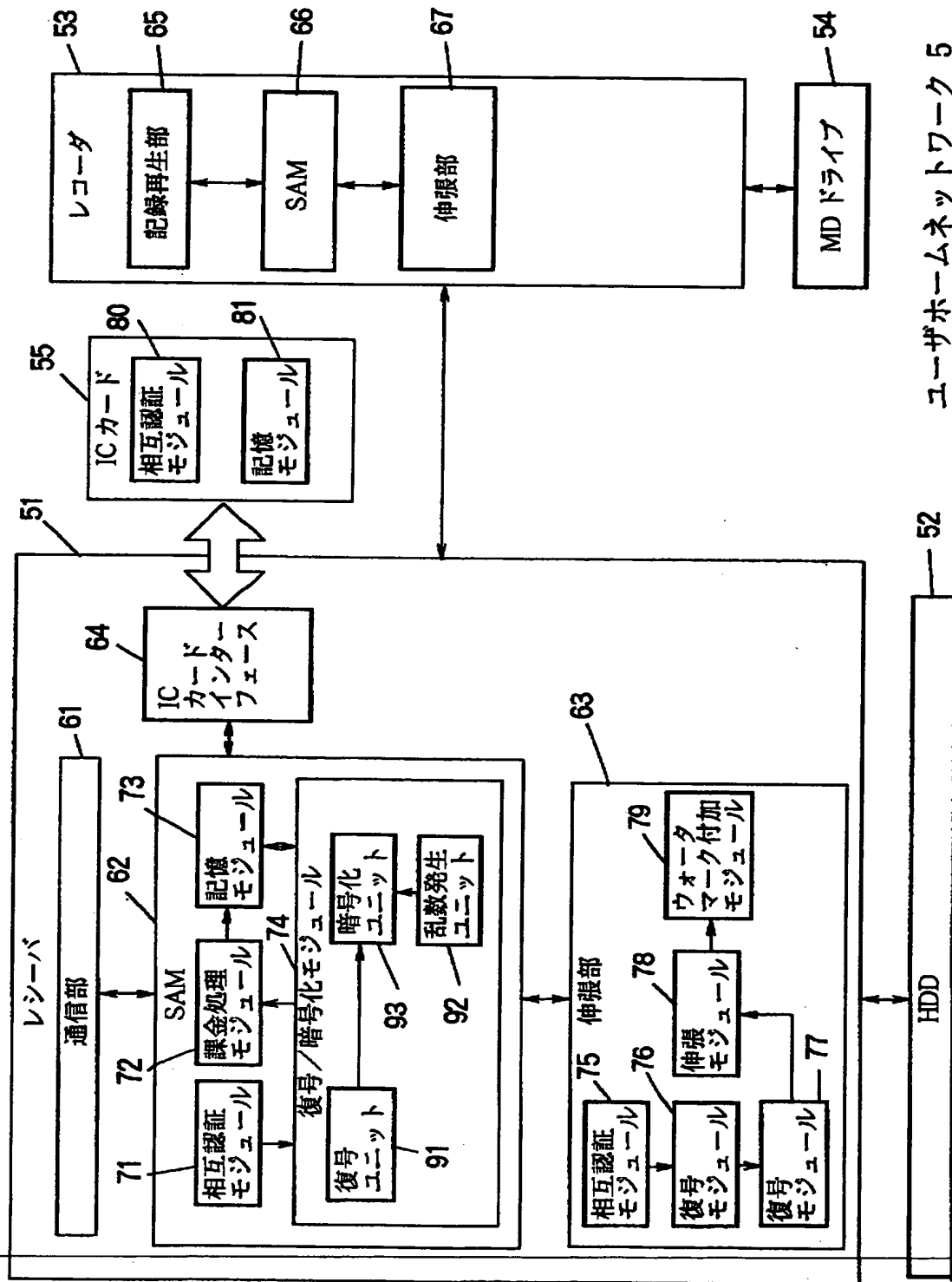
コンテンツプロバイダ 2

【図9】

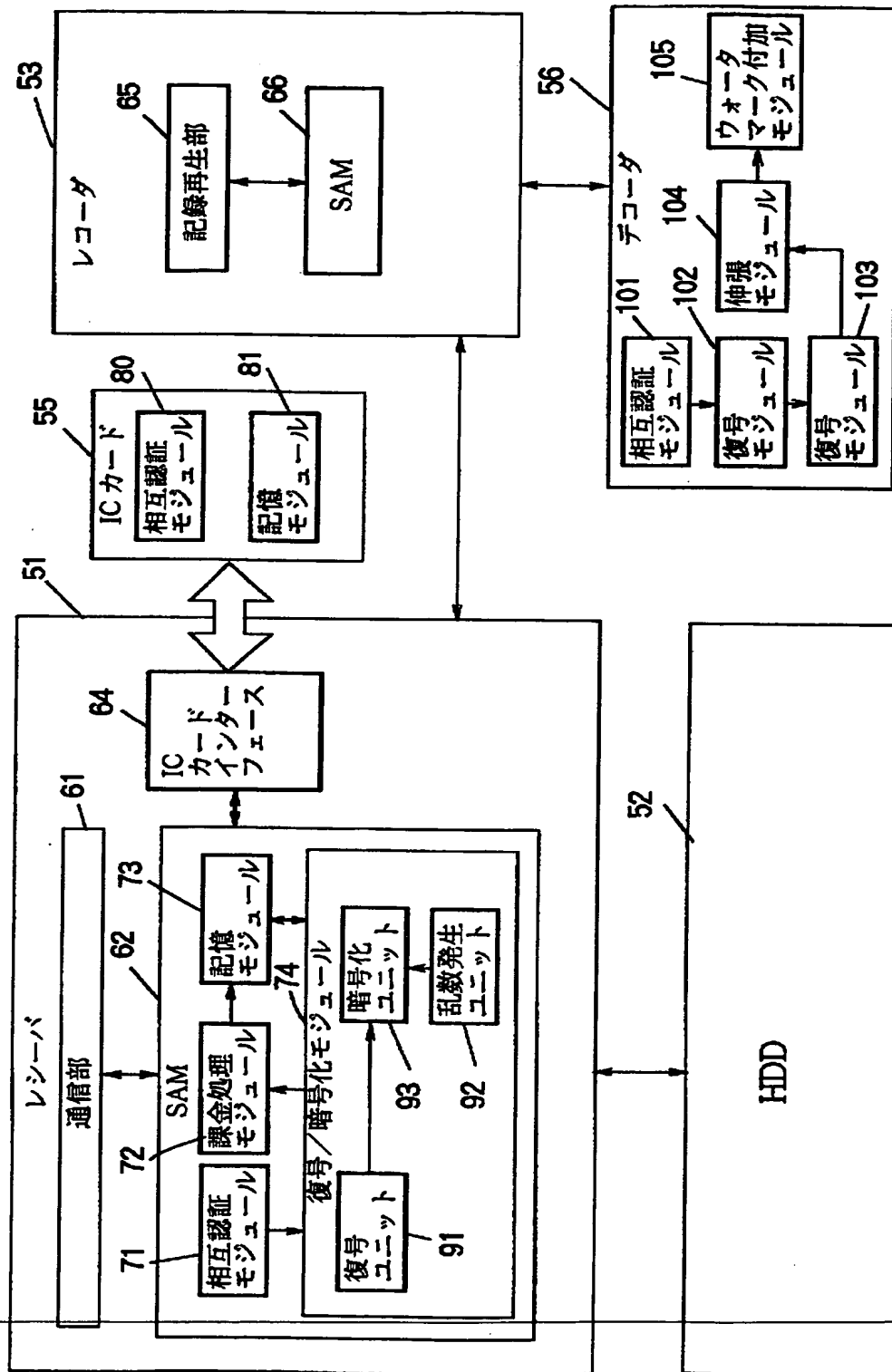


サービスプロバイダ 3

【図 10】

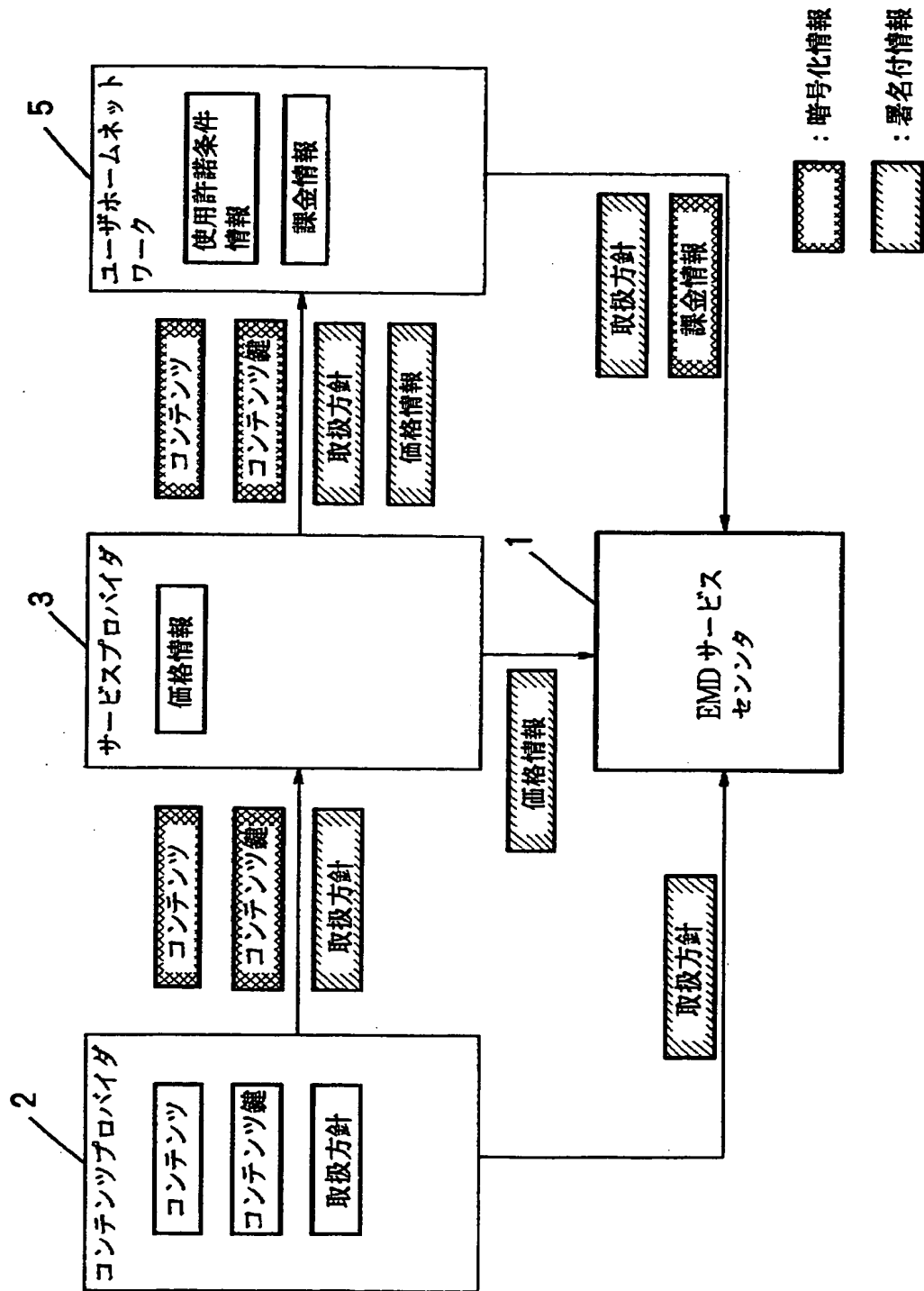


【図11】

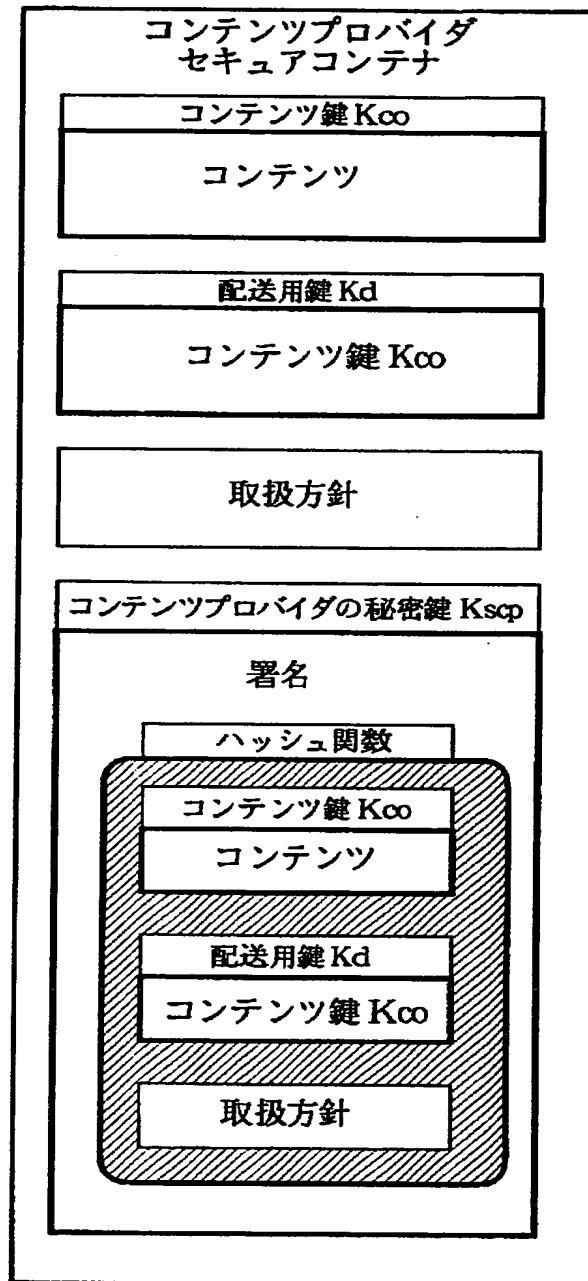


ユーザホームネットワーク 5

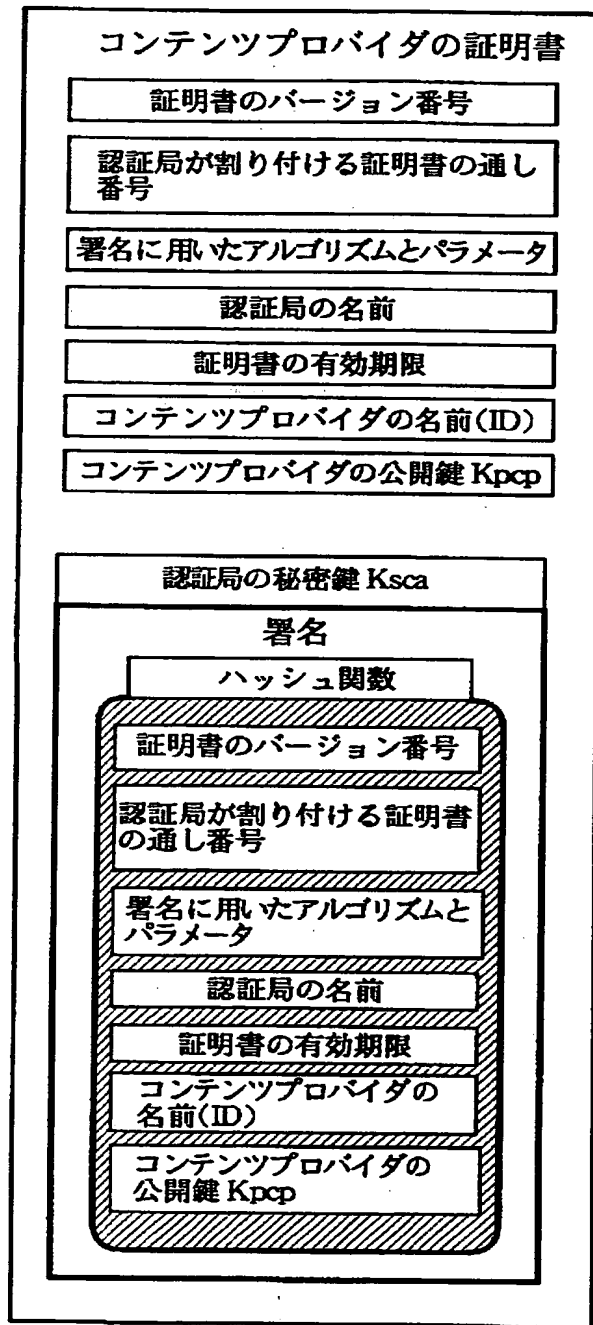
【図 12】



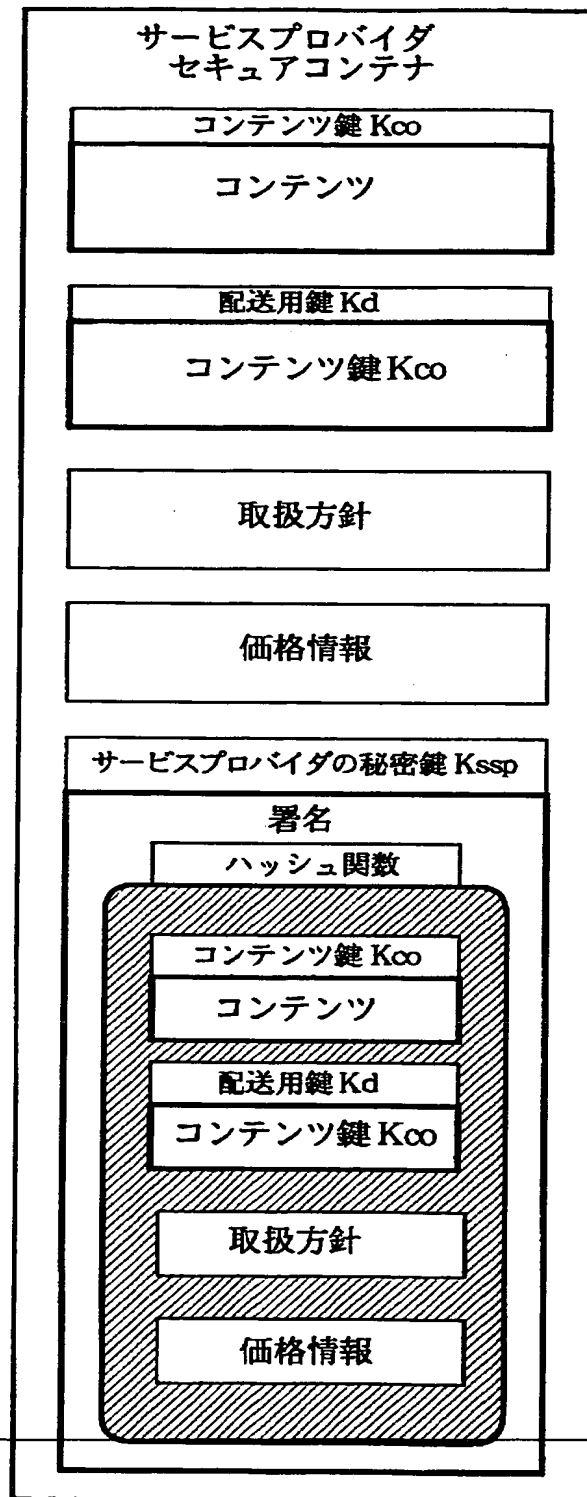
【図 13】



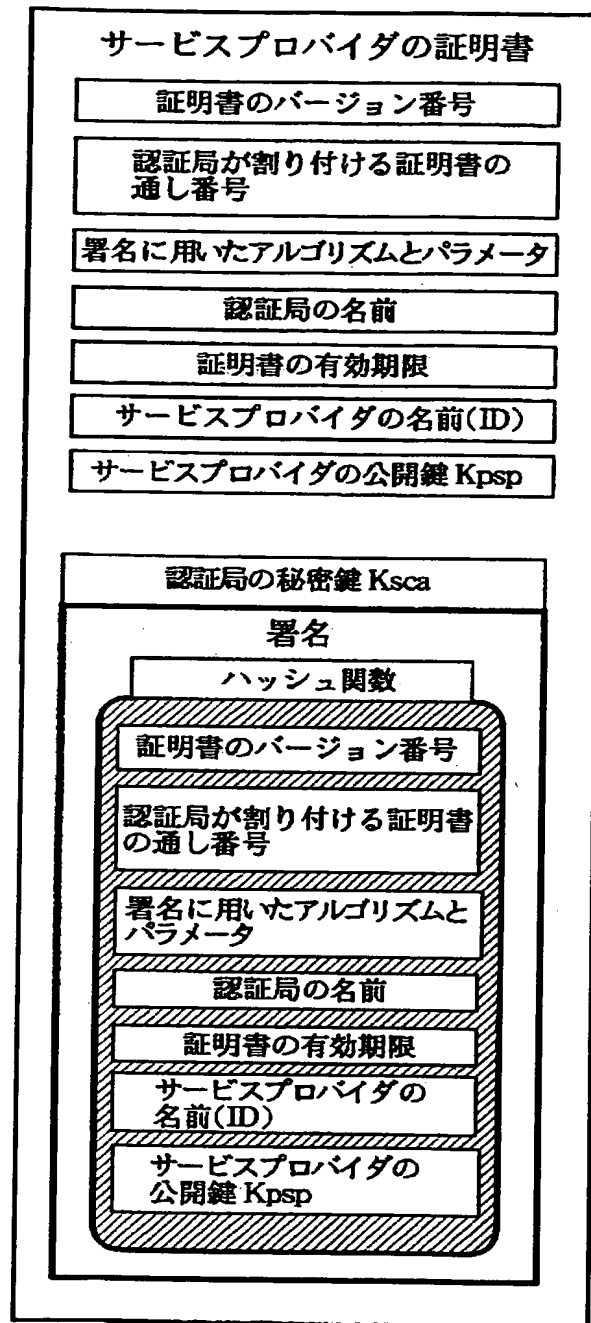
【図 14】



【図 15】



【図 16】

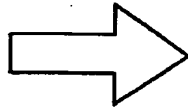


【図 17】

利用内容	再生	シングルコピー	マルチコピー
可/否	1	0	1

取扱方針

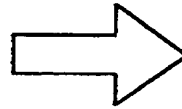
(A)



利用内容	再生	シングルコピー	マルチコピー
可/否	1	0	1
価格	150 円	-	80 円

取扱方針
および
価格情報

(B)

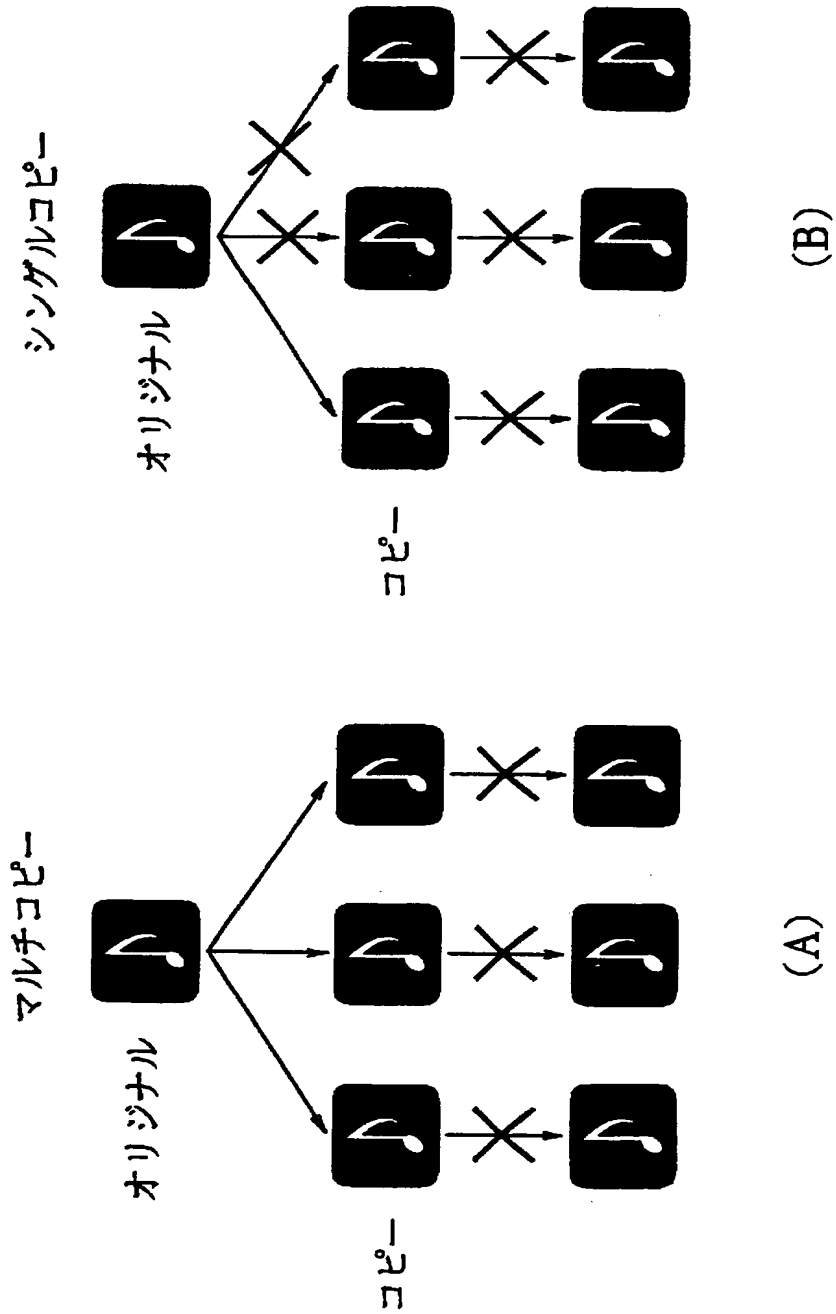


利用内容	再生	シングルコピー	マルチコピー
可/否	1	0	0

使用許諾
条件情報

(C)

【図 18】

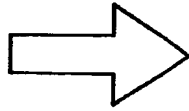


【図 1 9】

利用内容	再生	シングルコピー	マルチコピー
可/否	1	0	1
利益分配	70 円	-	40 円

取扱方針
利益分配

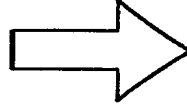
(A)



利用内容	再生	シングルコピー	マルチコピー
可/否	1	0	1
利益分配	60 円	-	30 円
分配価格	150 円	-	80 円

取扱方針
利益分配
価格情報

(B)



利用内容	再生	シングルコピー	マルチコピー
利用回数	1	0	0

課金情報

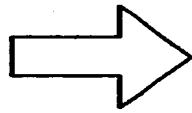
(C)

【図 20】

利用内容	再生		
	制限なし	回数制限	期日制限
	-	5	1998/12/31
価格	-	60 円	90 円

取扱方針
および
価格情報

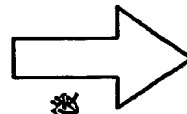
(A)



利用内容	再生		
	制限なし	回数制限	期日制限
	-	5	-

使用許諾条件
情報

(B)



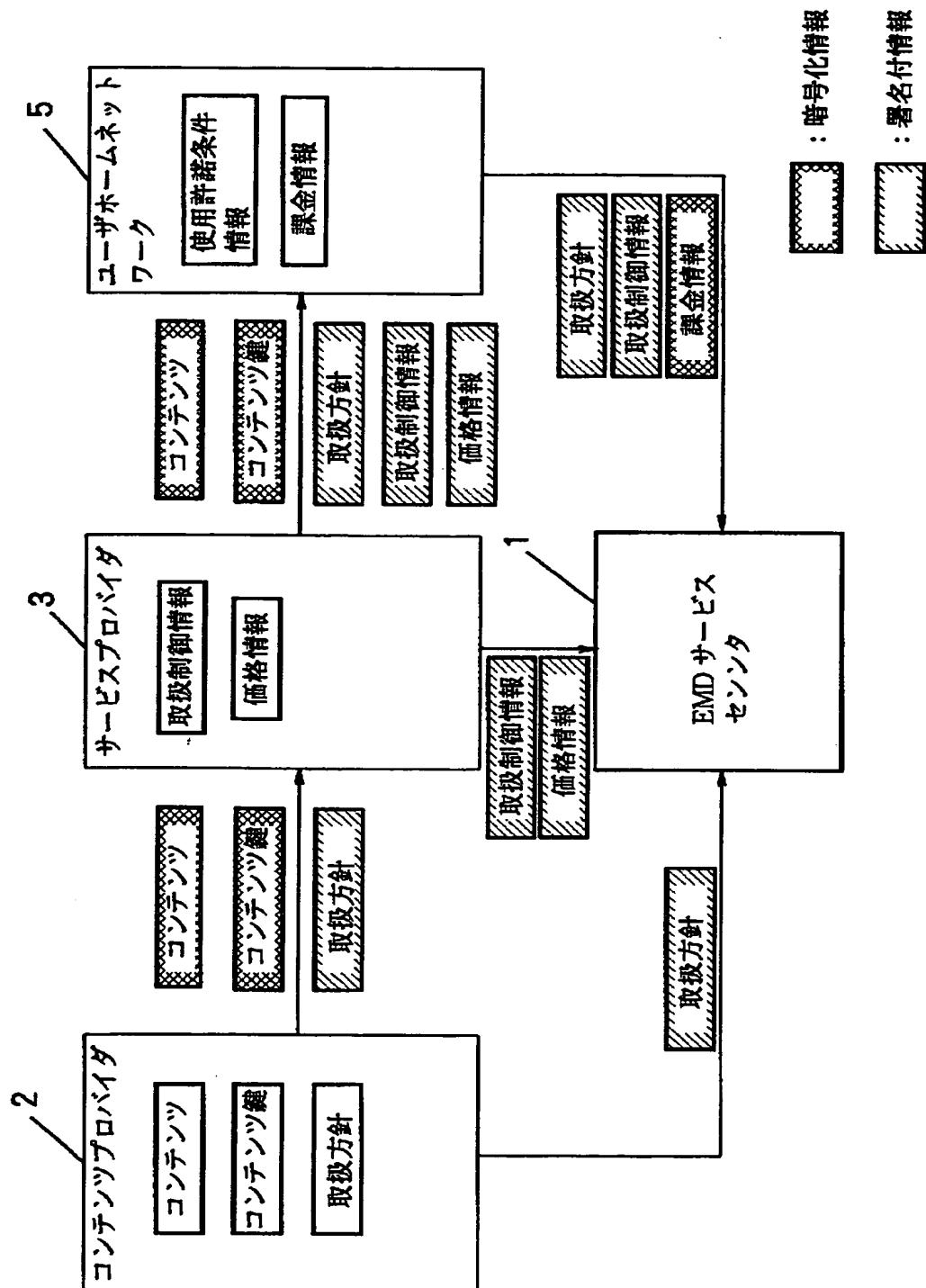
3回再生後

利用内容	再生		
	制限なし	回数制限	期日制限
	-	2	-

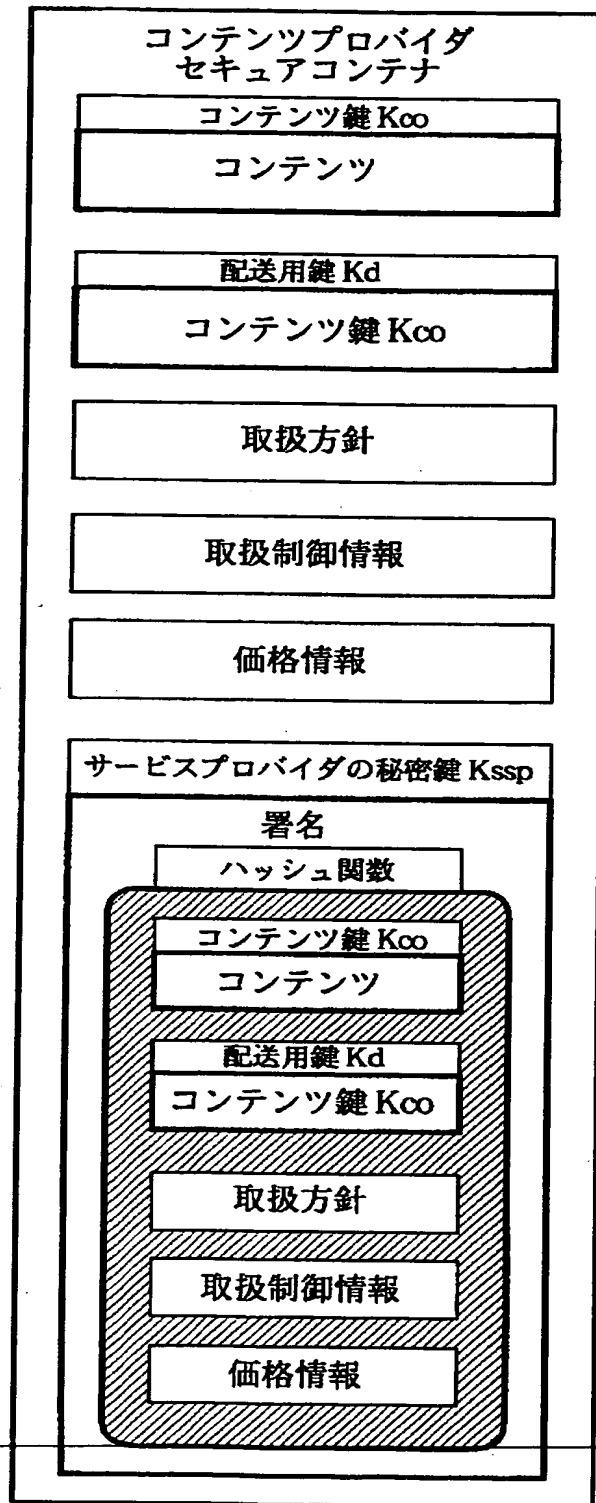
使用許諾条件
情報

(C)

【図 21】



【図 22】



【図 2 3】

再生：YES；
シングルコピー：NO；
マルチコピー：YES

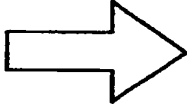
(A) 取扱方針



利用内容	再生	シングルコピー	マルチコピー
可／否	1	0	1
価格	150 円	-	80 円

取扱制御情報
および
価格情報

(B)

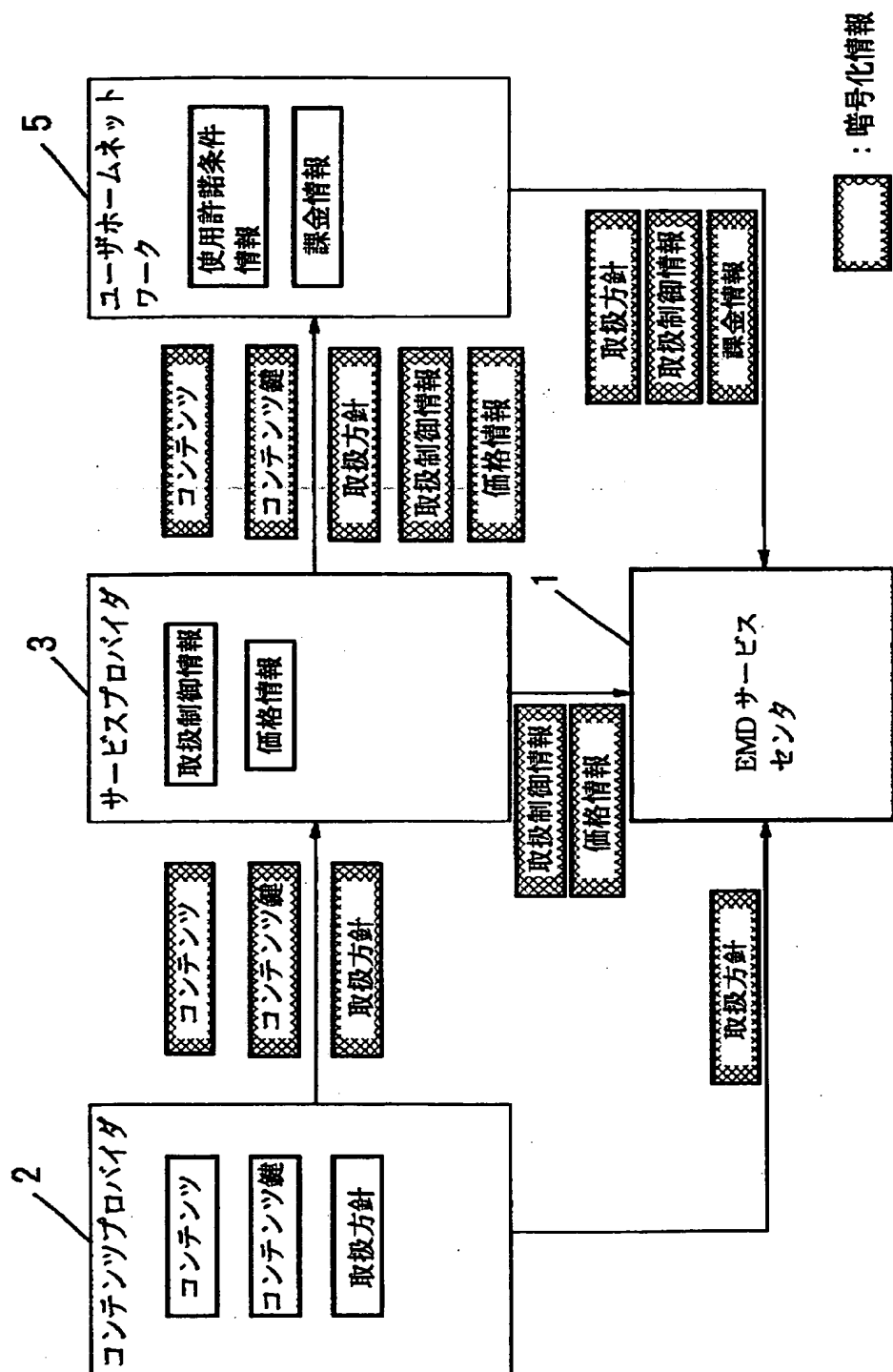


利用内容	再生	シングルコピー	マルチコピー
可／否	1	0	0

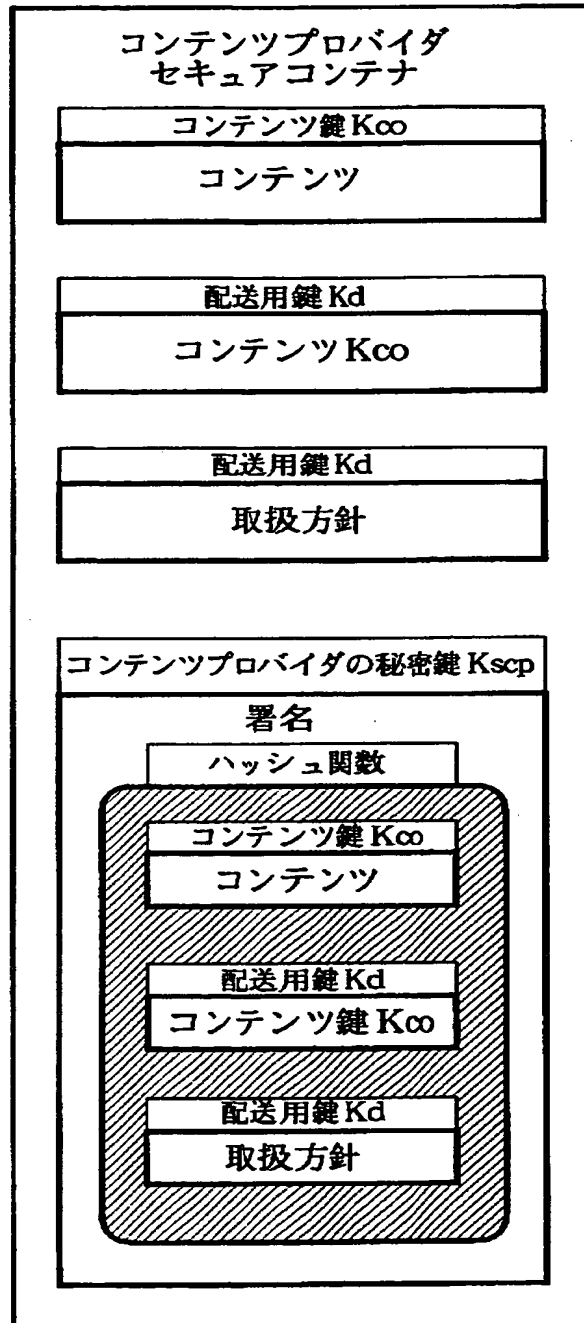
使用許諾
条件情報

(C)

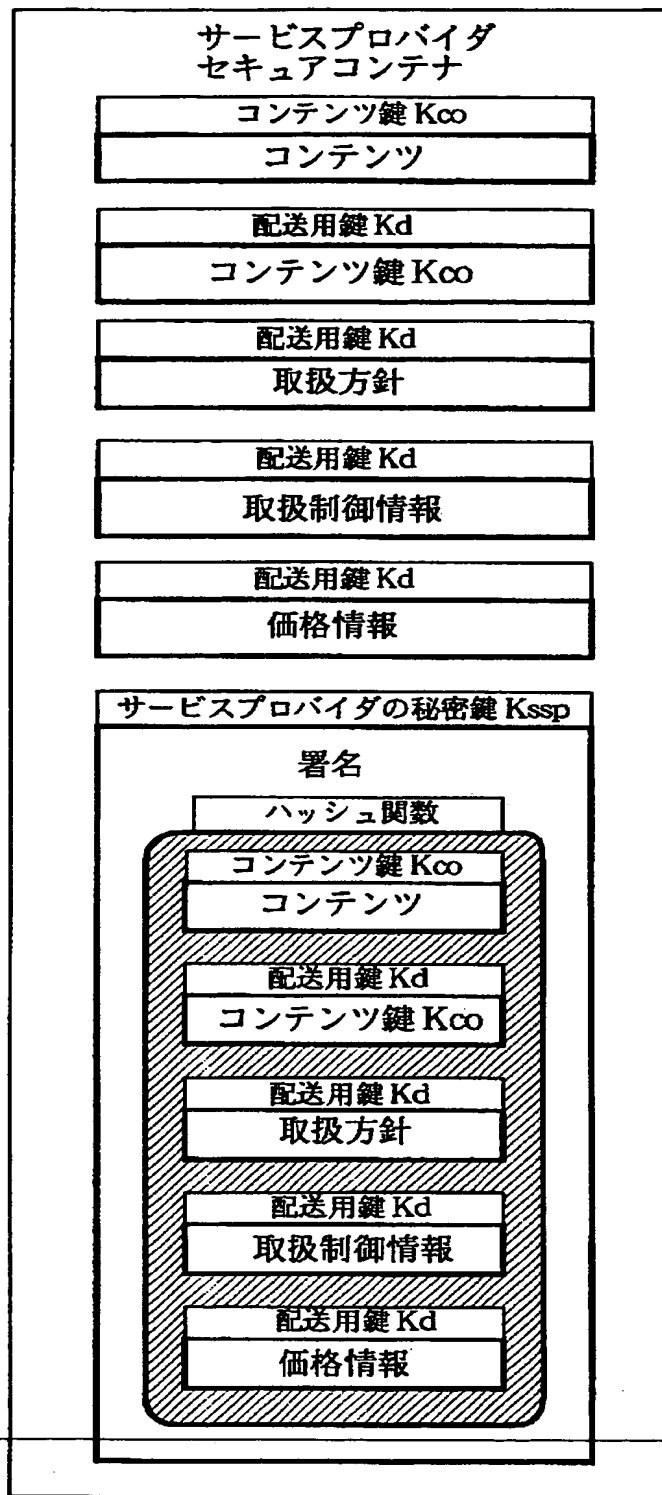
【図 24】



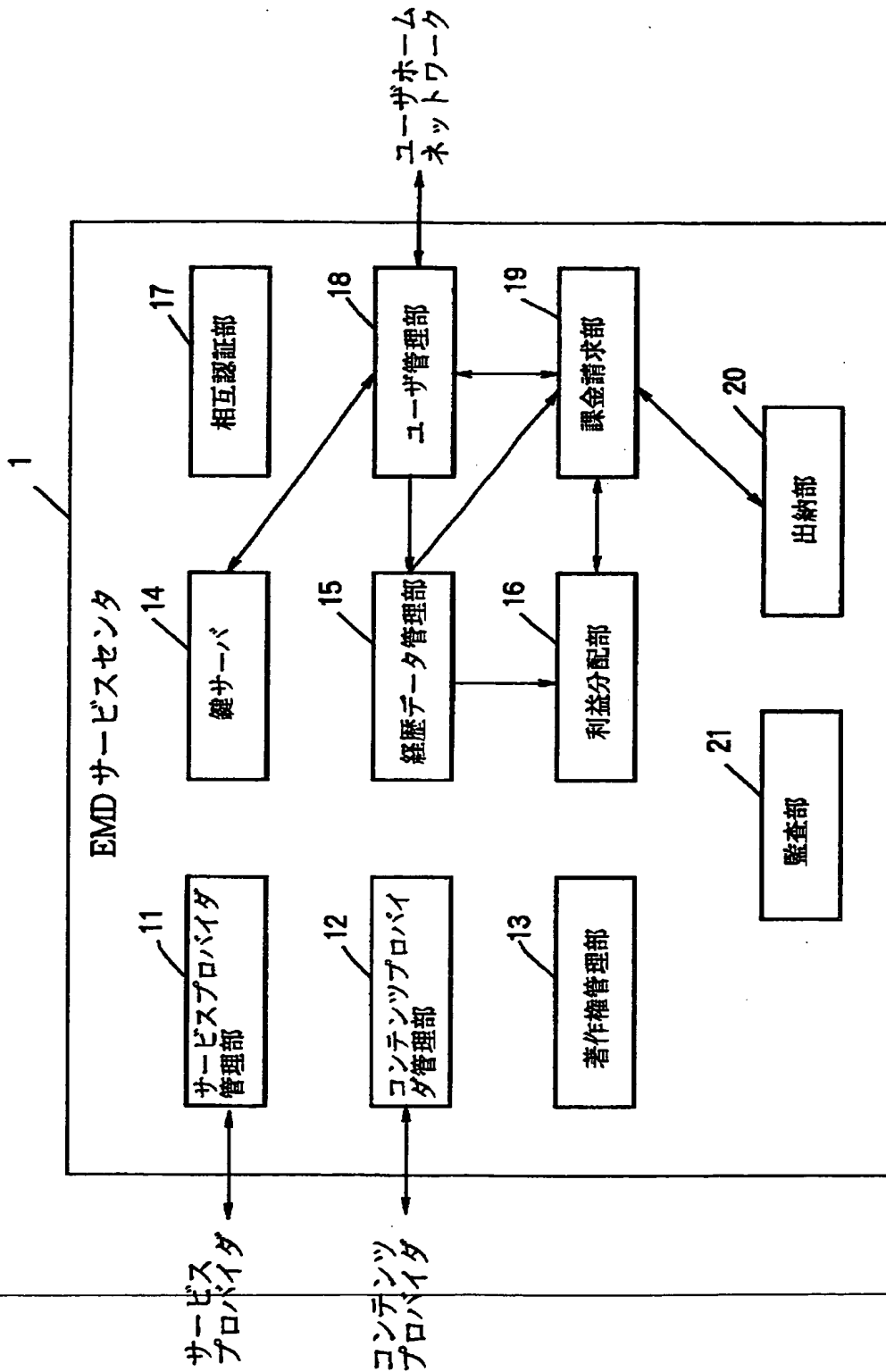
【図 25】



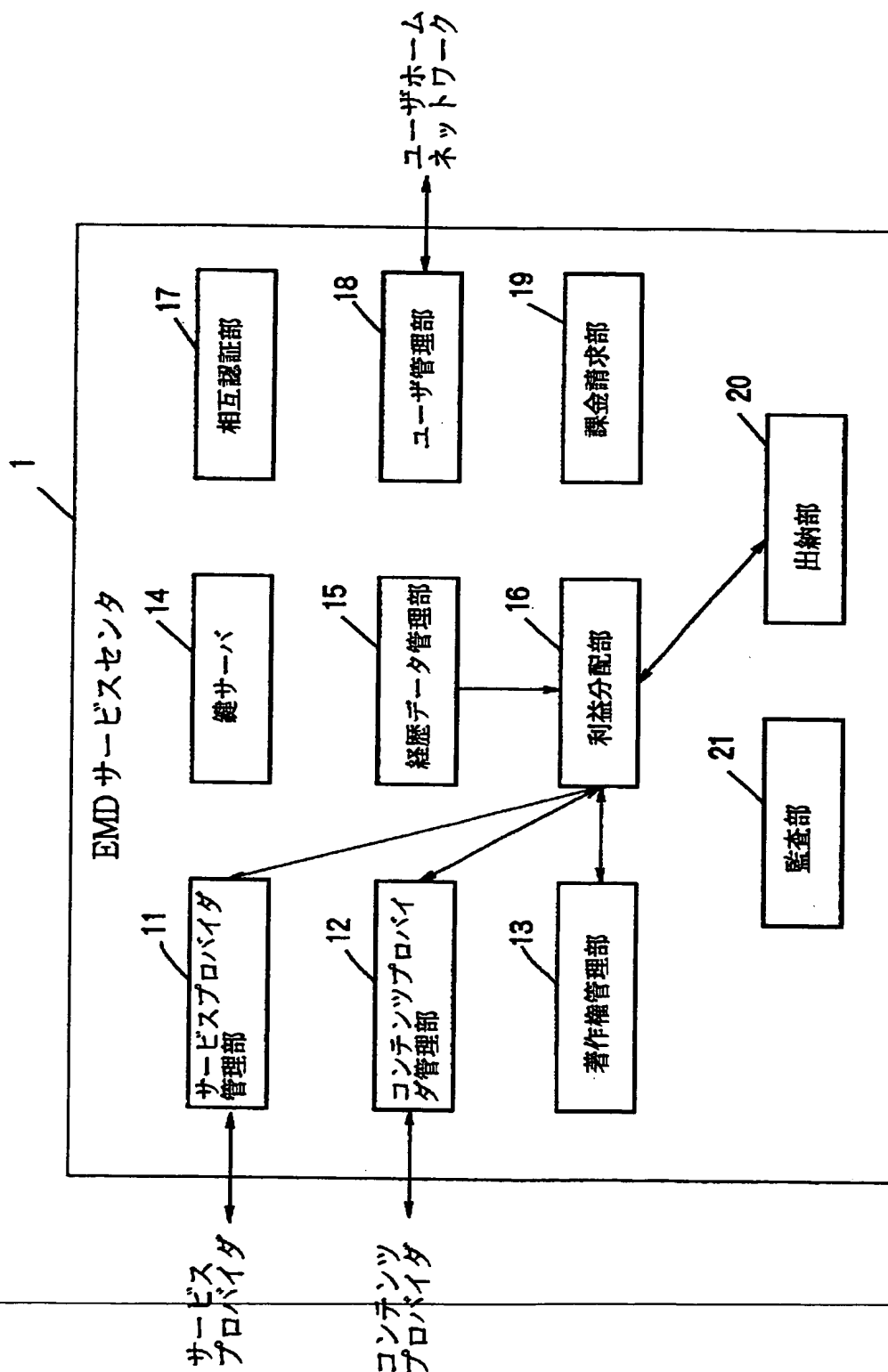
【図 26】



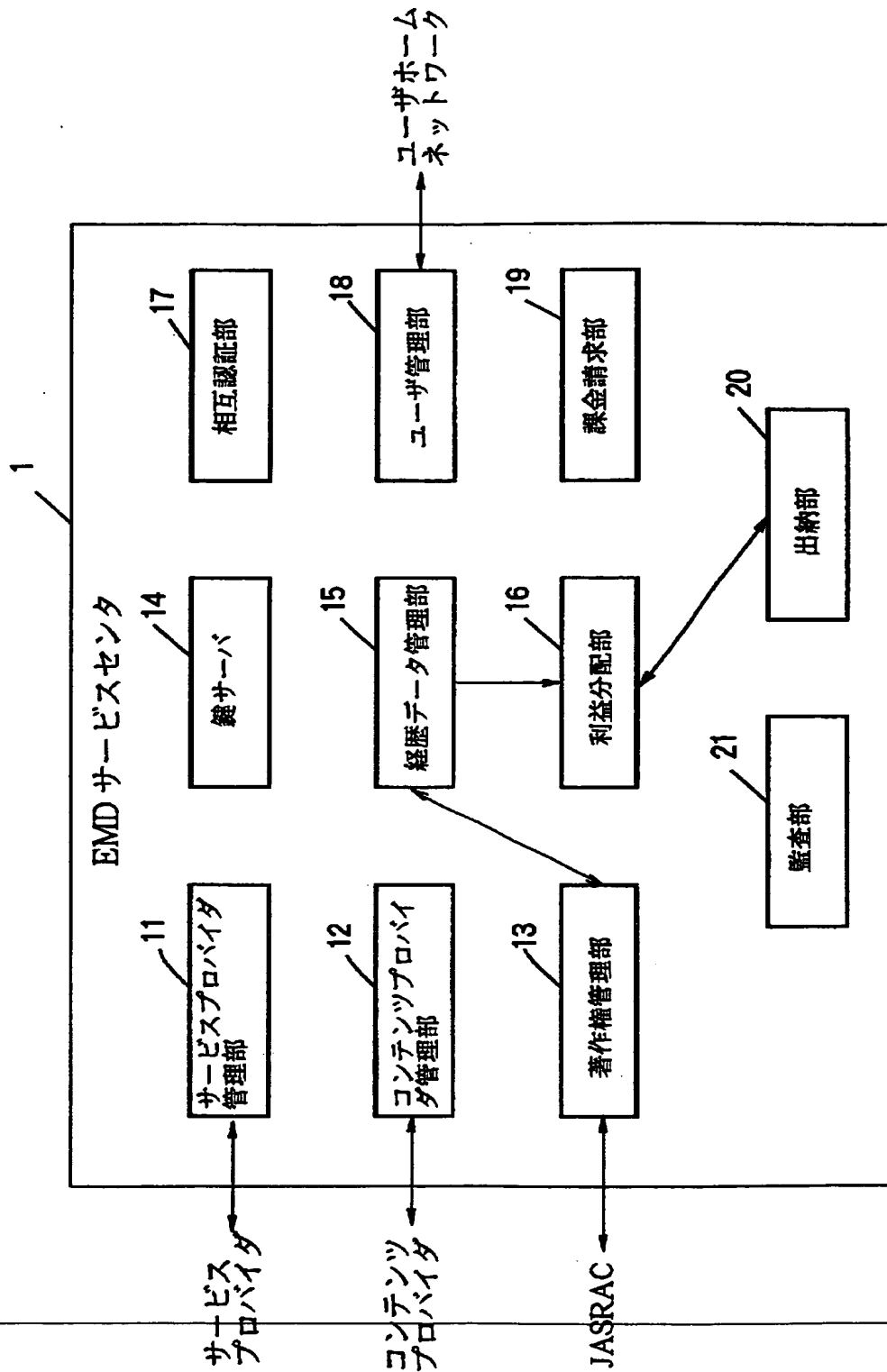
【図 27】



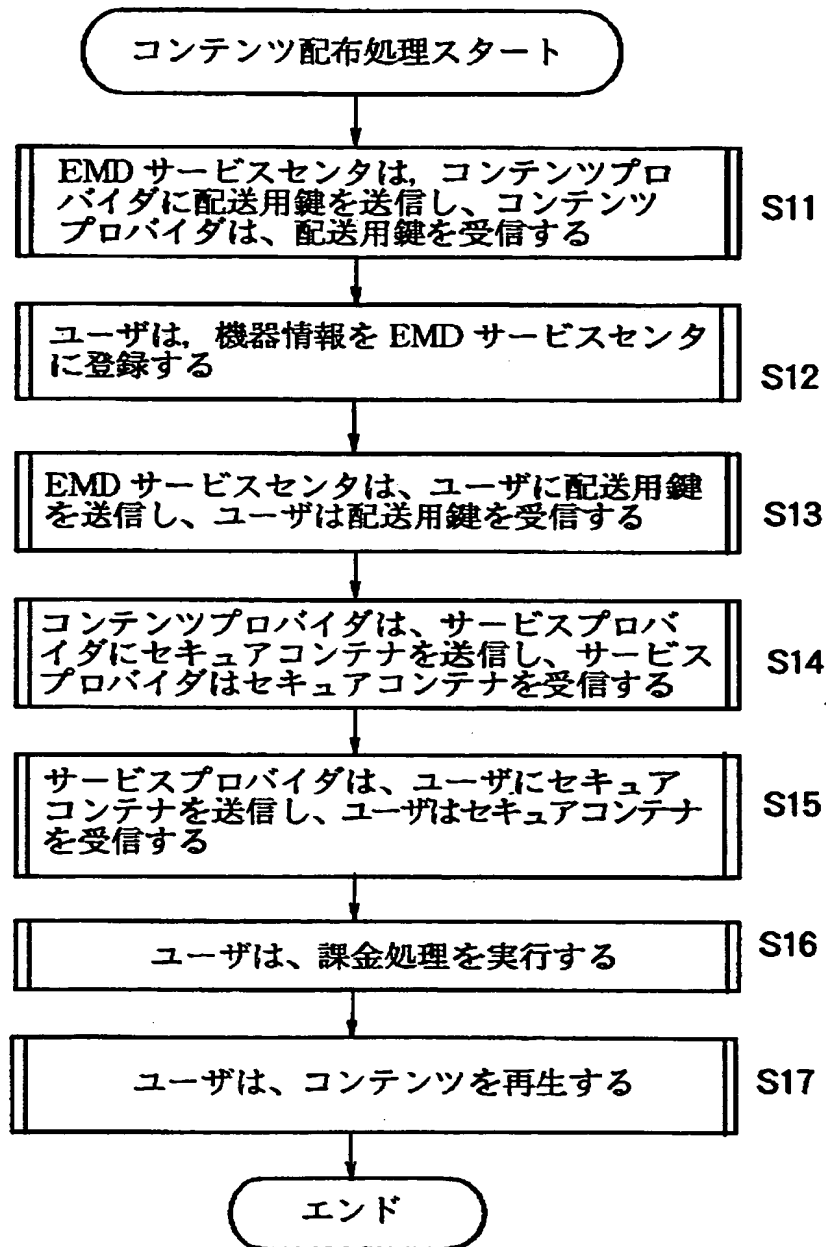
【図28】



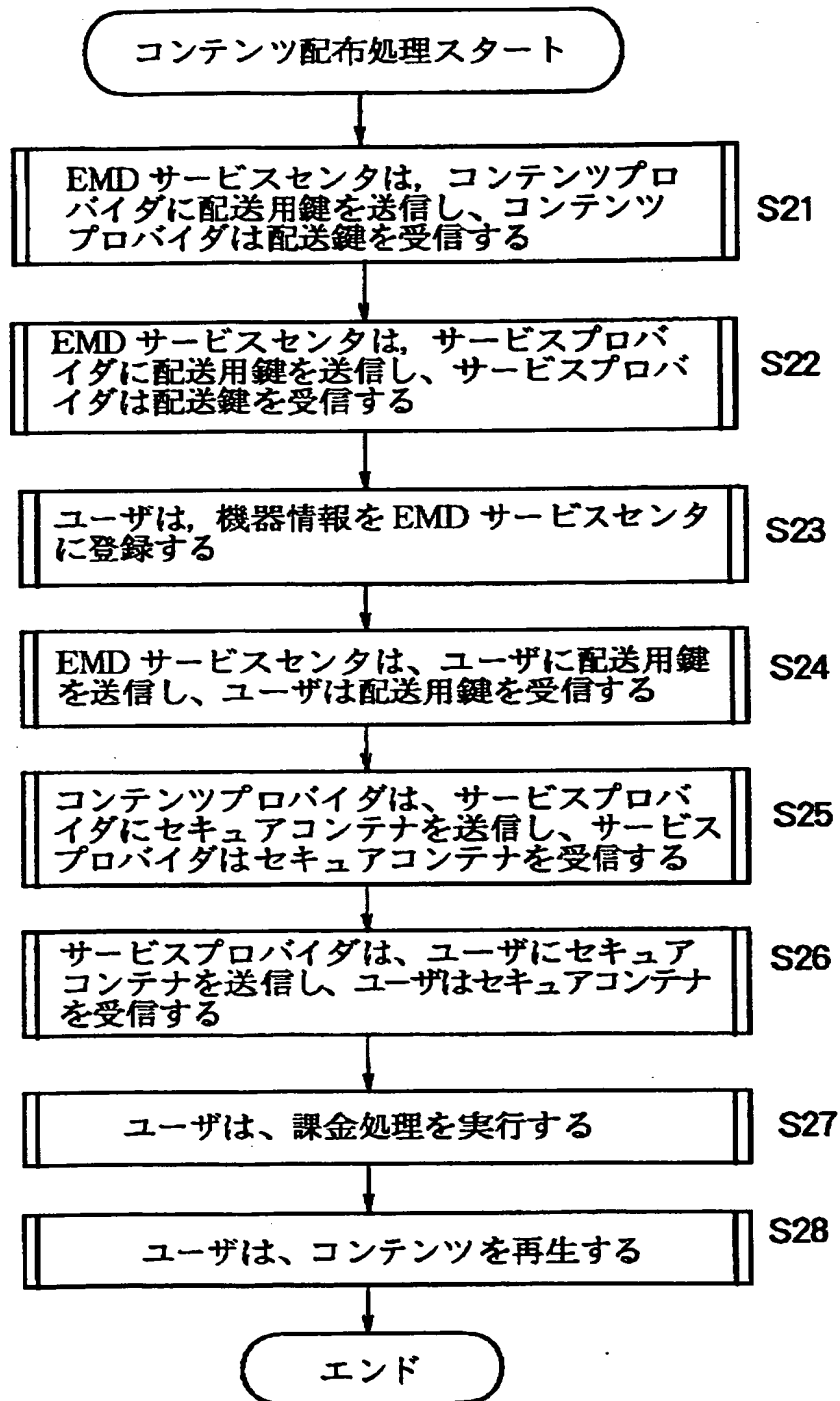
【図 29】



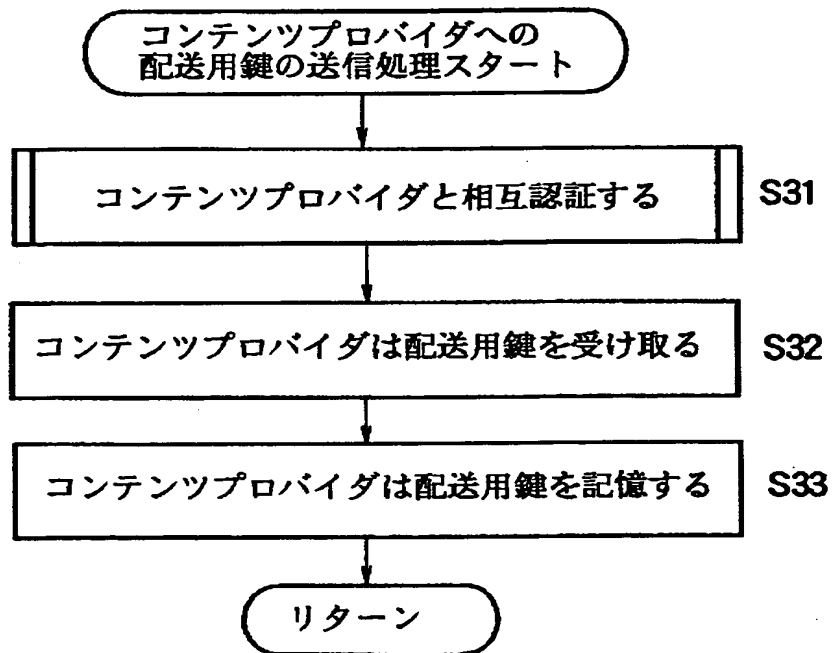
【図 30】



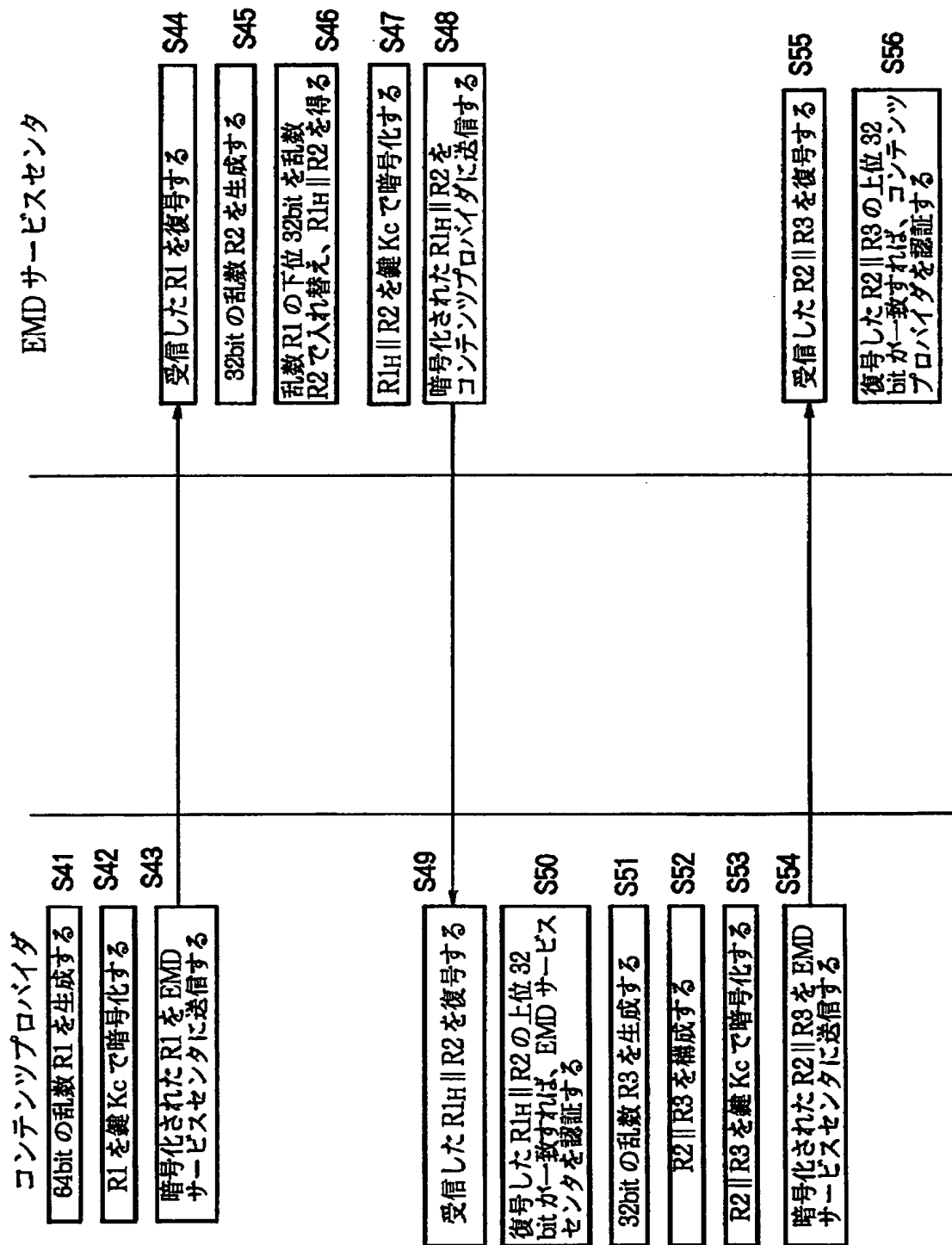
【図 31】



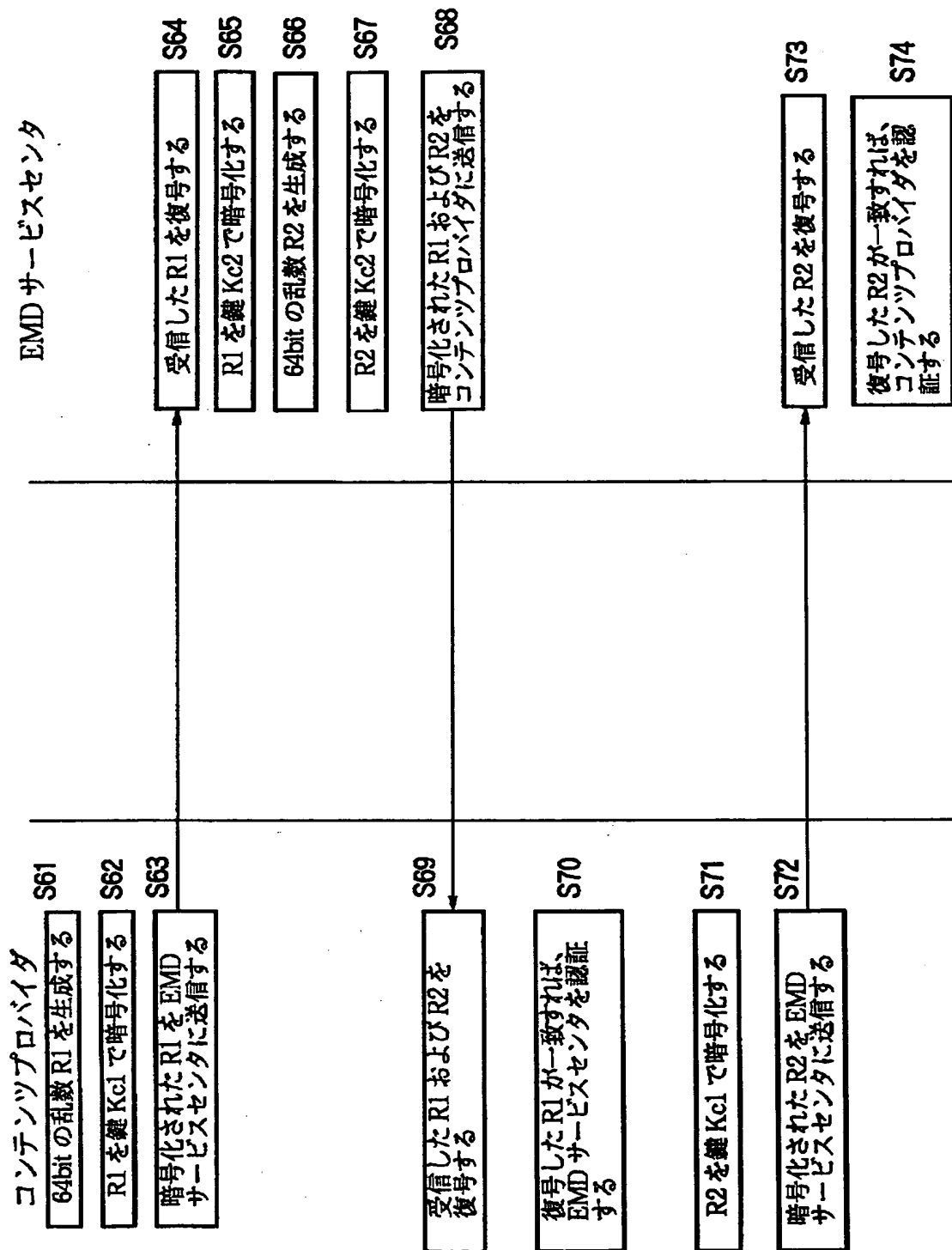
【図 32】



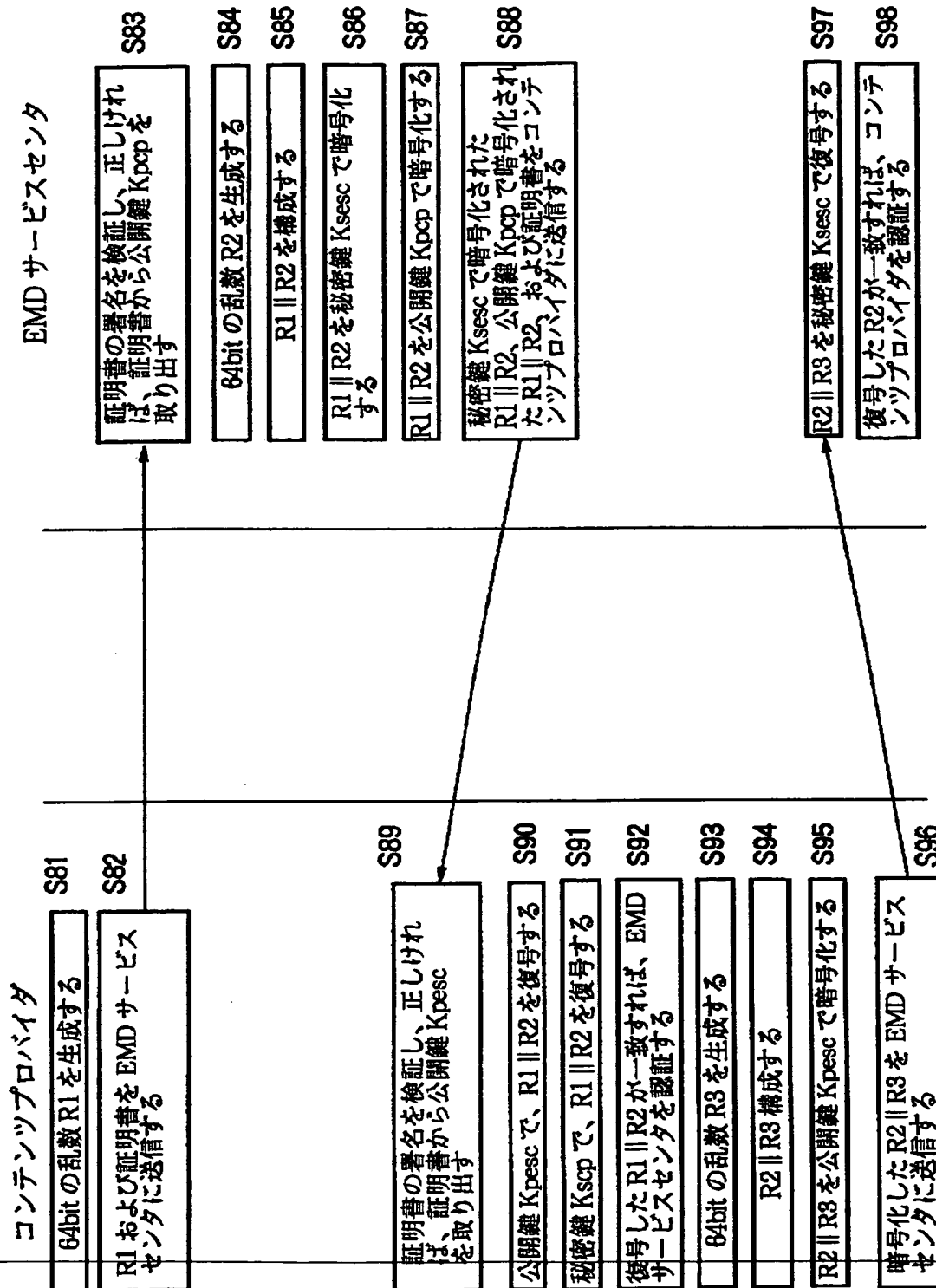
【 図 3 3 】



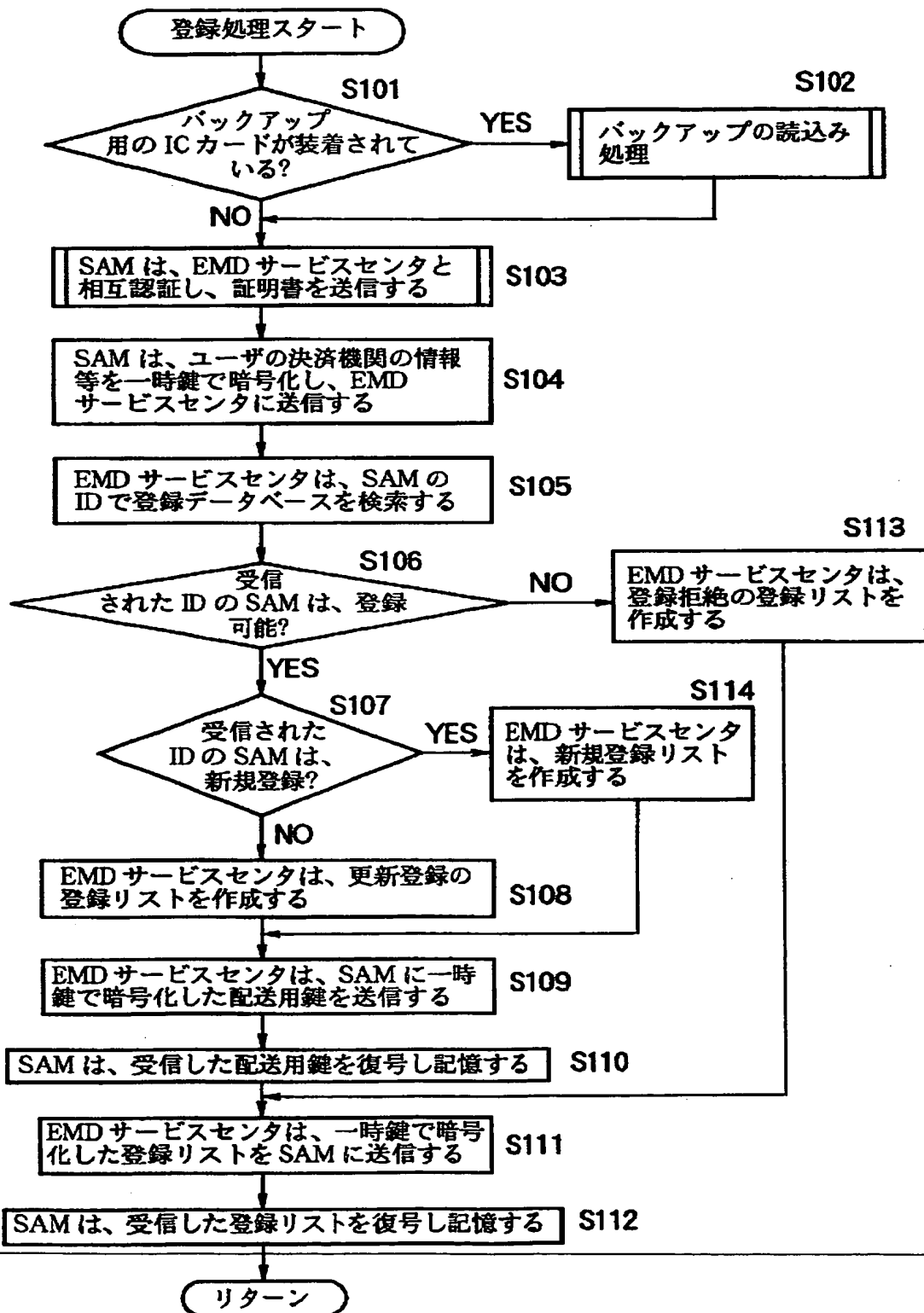
【図 34】



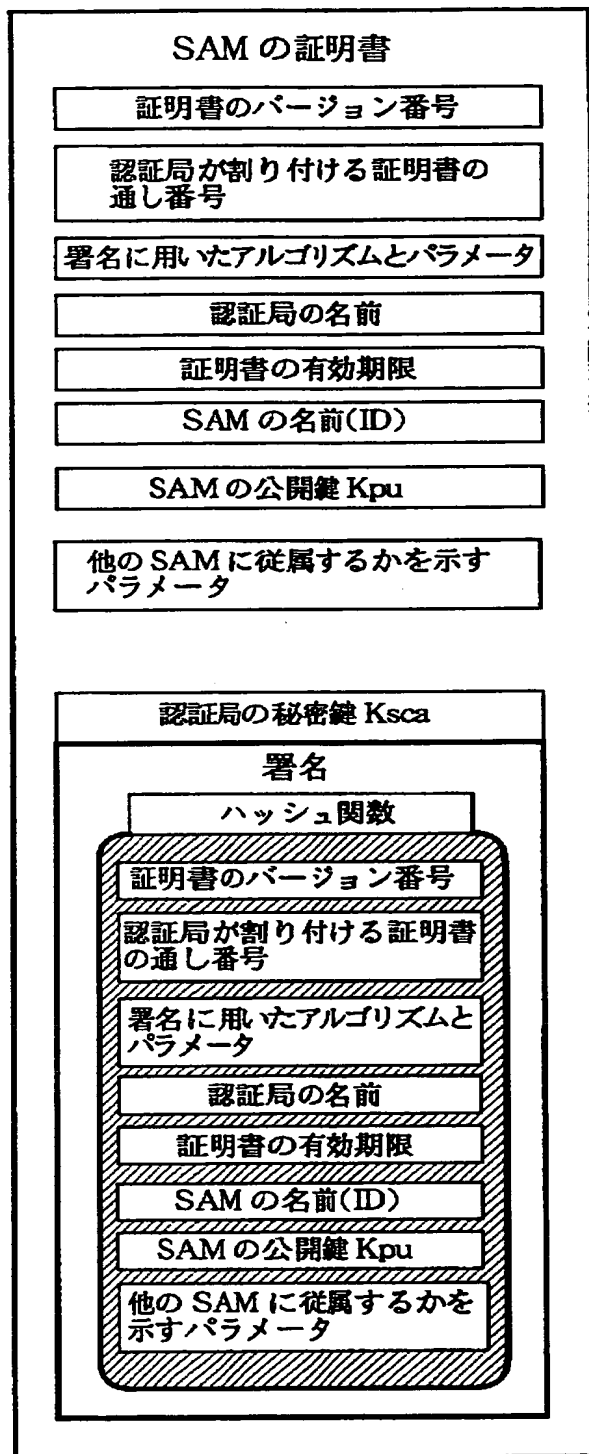
【図 3 5】



【図 36】



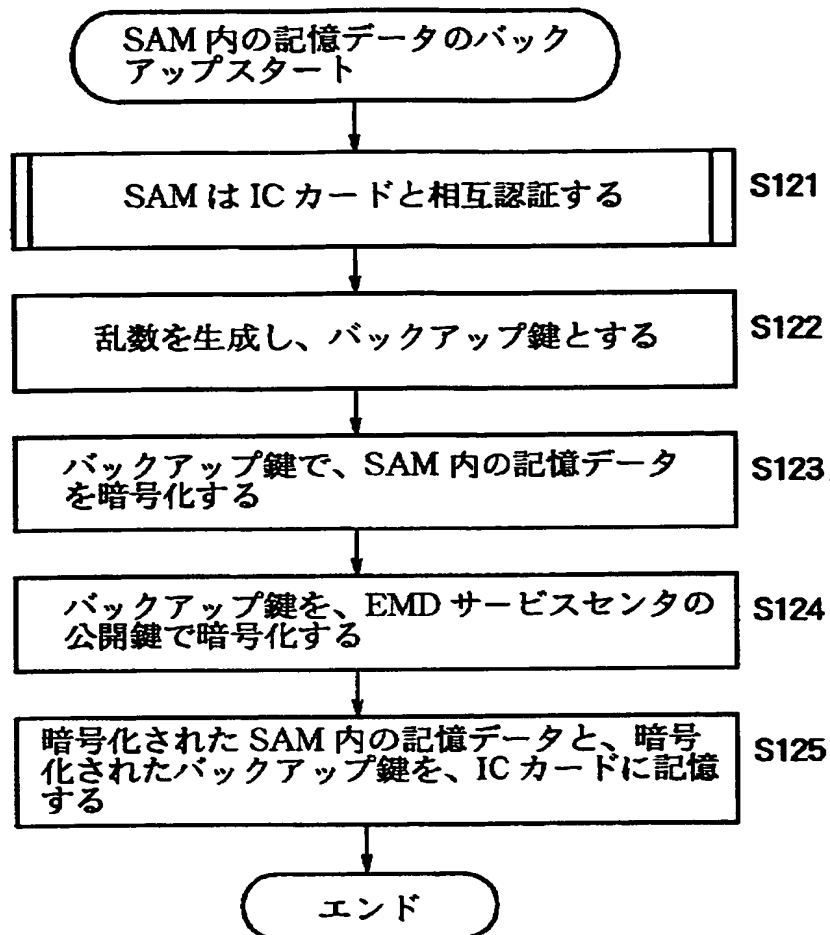
【図 37】



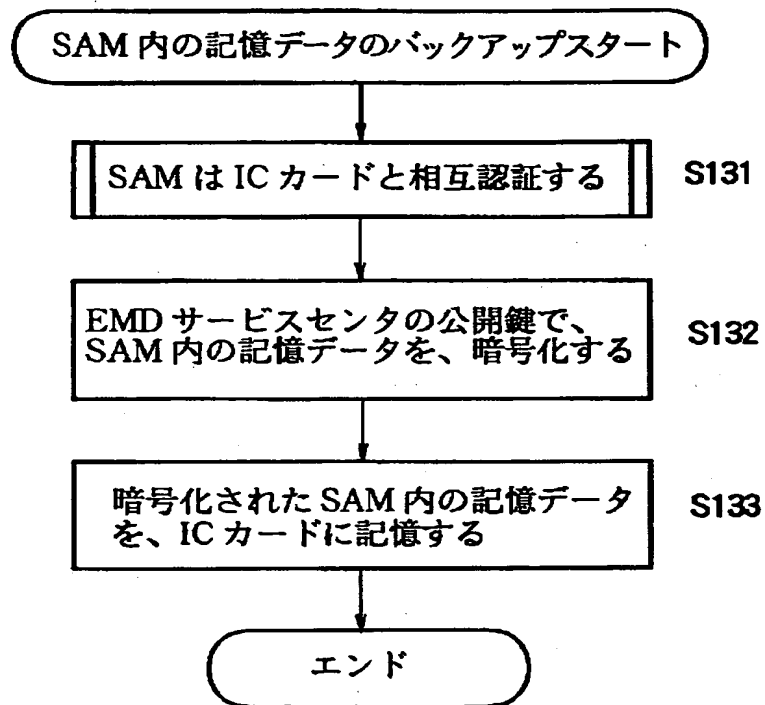
【图 3 8】

SAM の ID (64bit)	登録拒絶フラグ (1bit)	ステータスフラグ (4bit)	コンディションフラグ (1bit)	署名
0000000000000001h	1	0000	0	xxxxxxxxxx
0000000000000002h	1	1010	1	xxxxxxxxxx
0000000000000003h	1	1100	1	xxxxxxxxxx
0000000000000000Ah	0	0000	1	xxxxxxxxxx

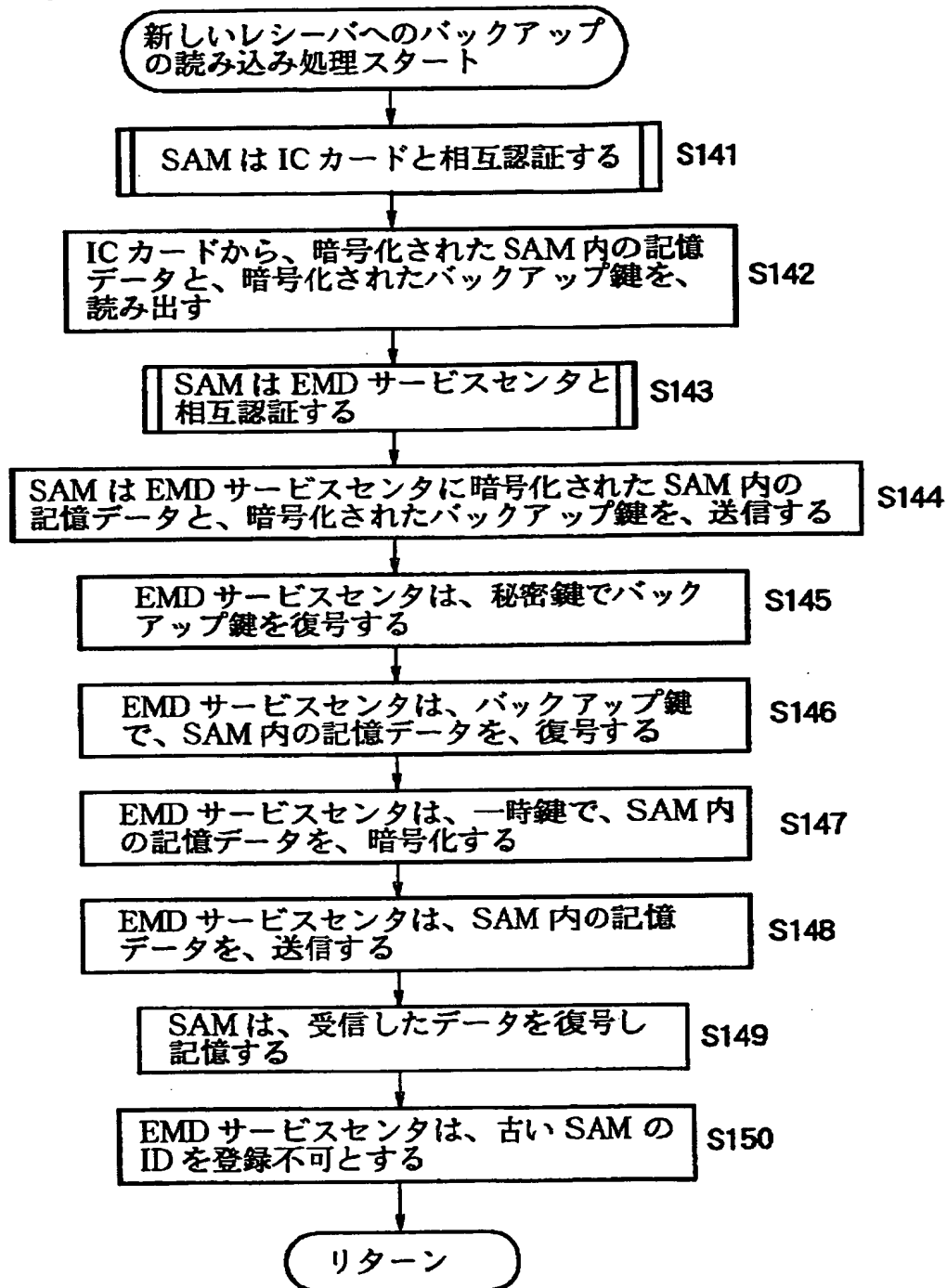
【図 39】



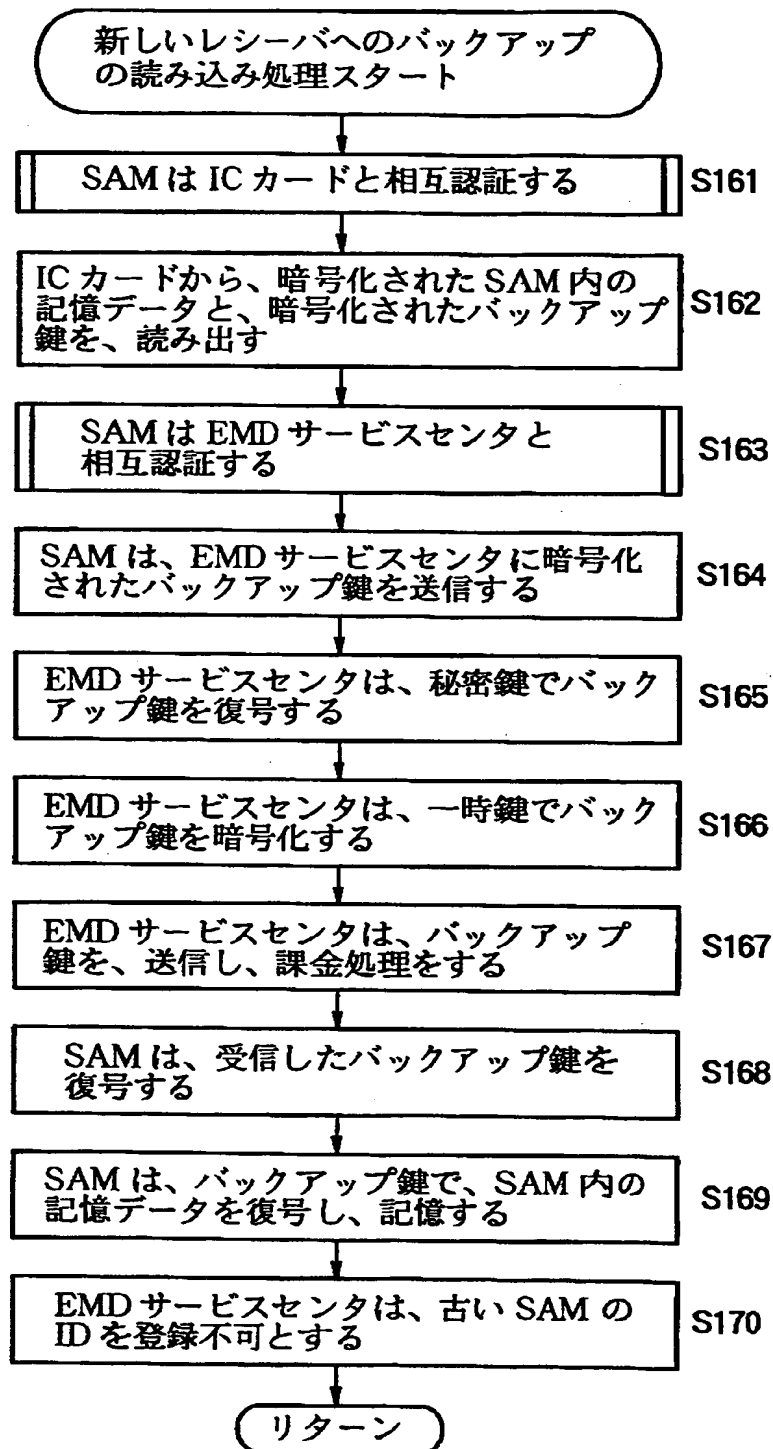
【図 40】



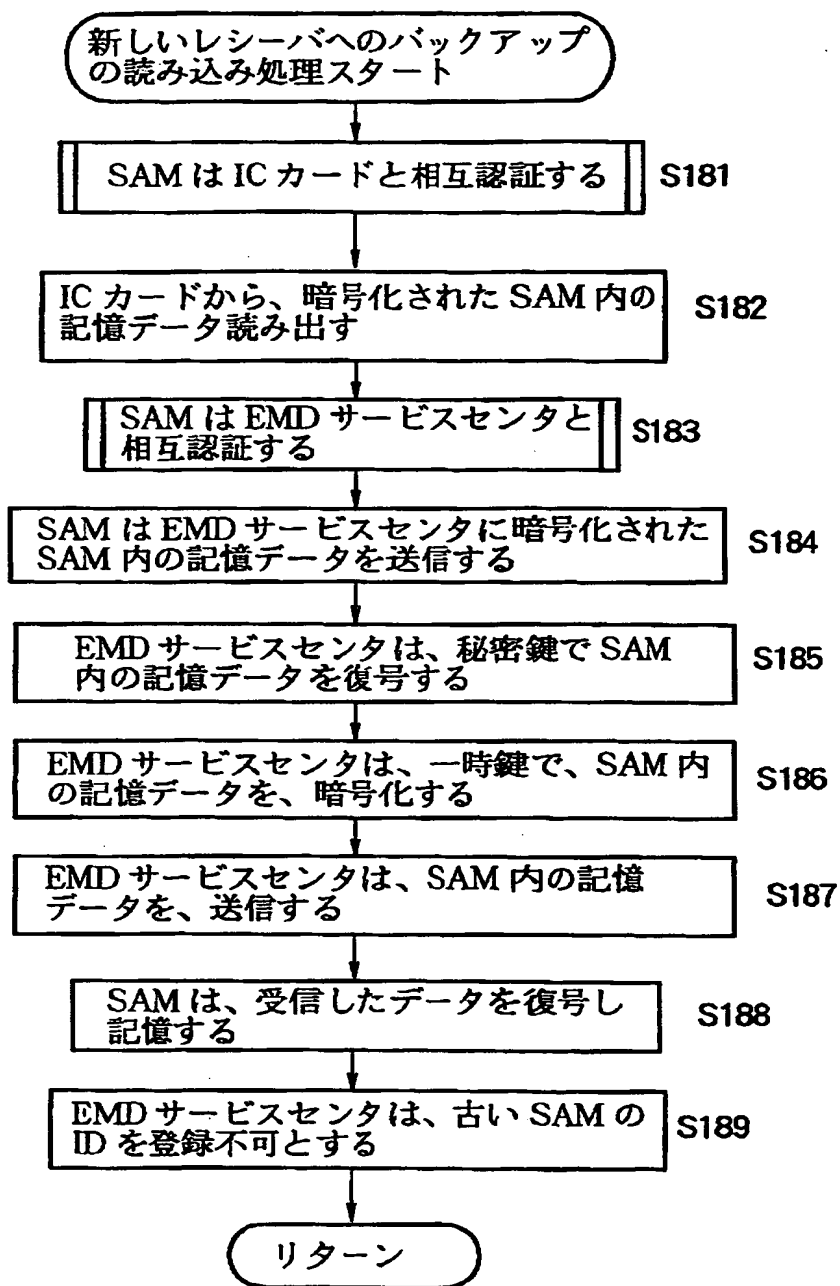
【図 4 1】



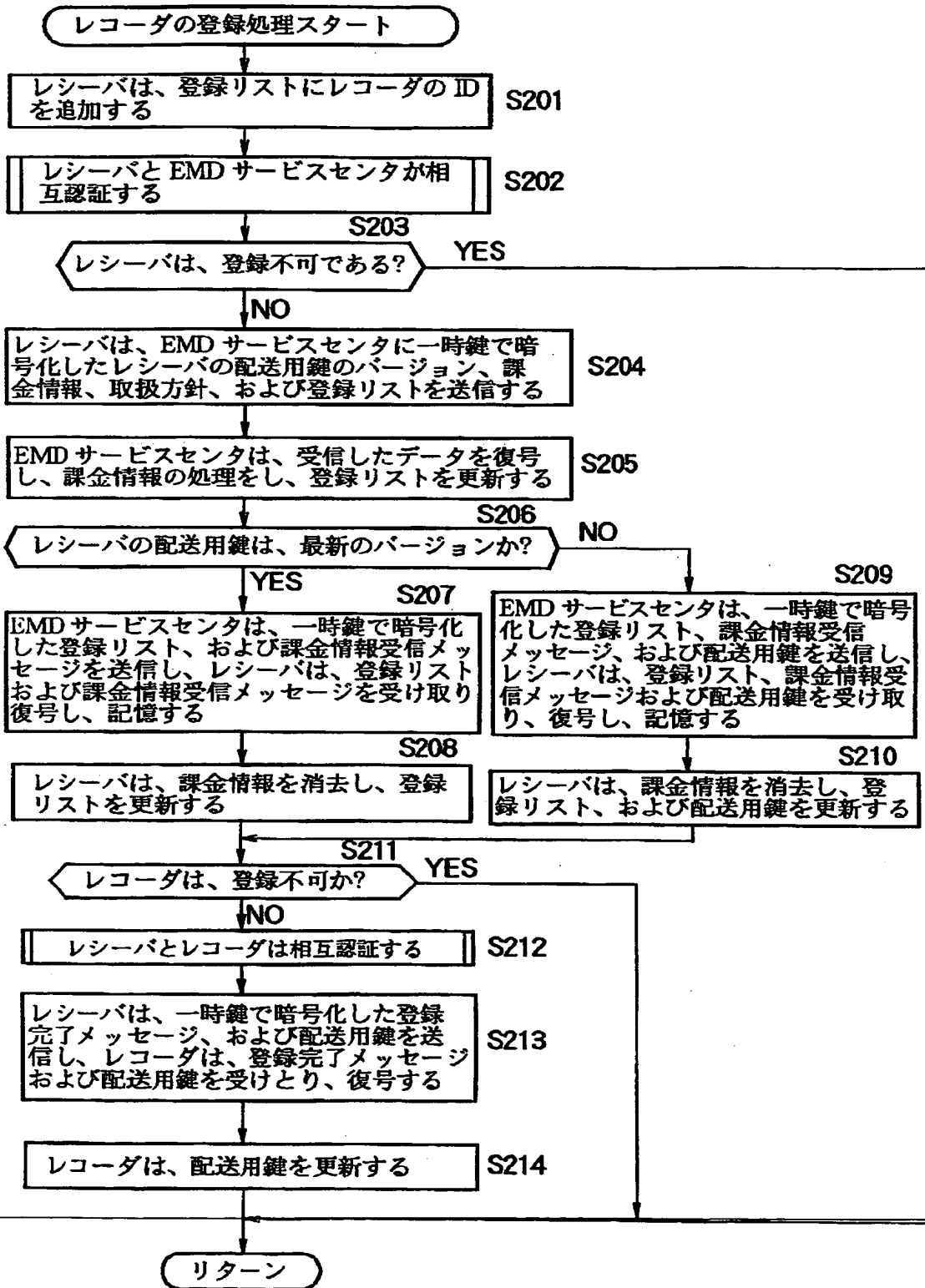
【図 4 2】



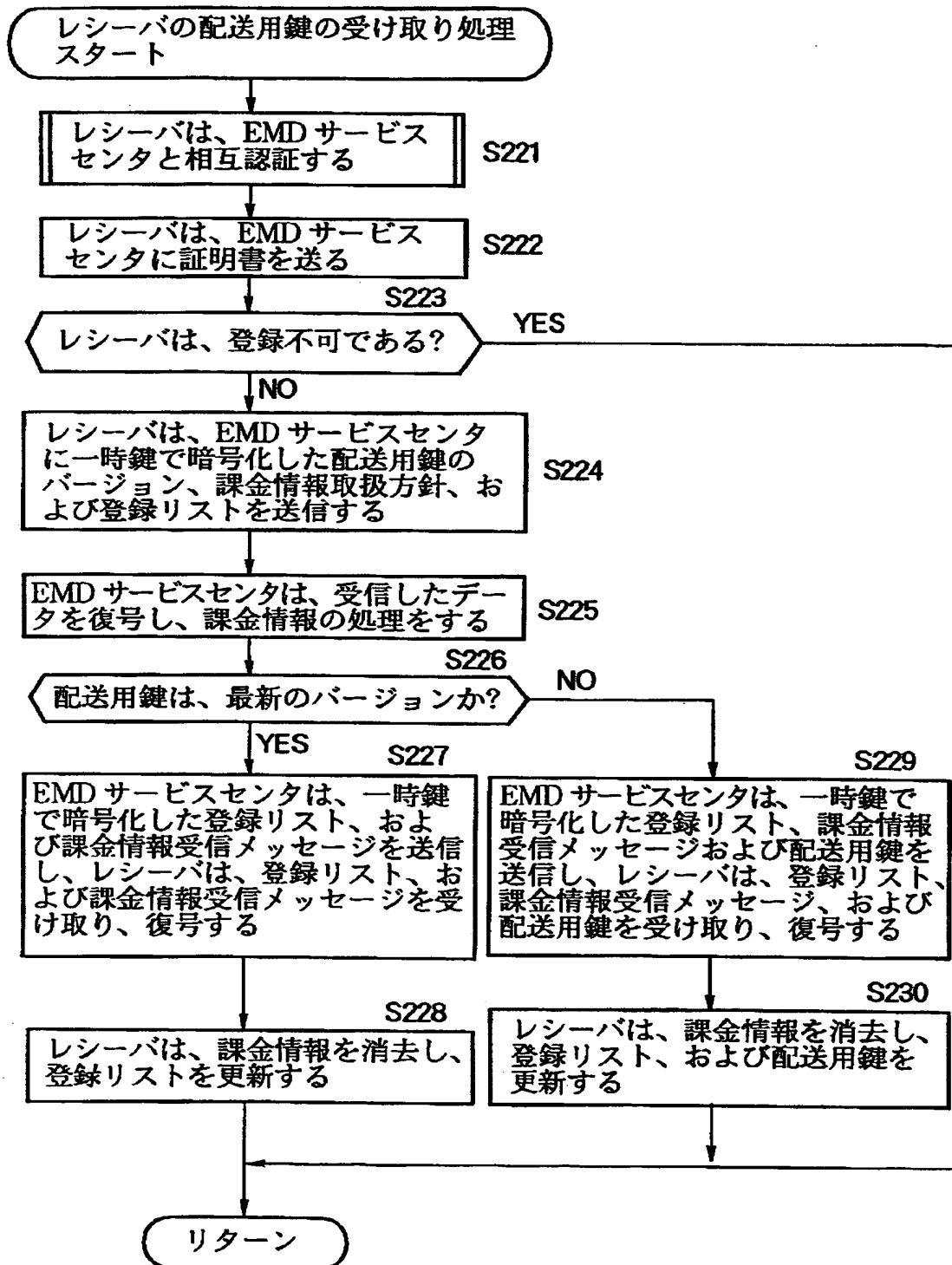
【図 4 3】



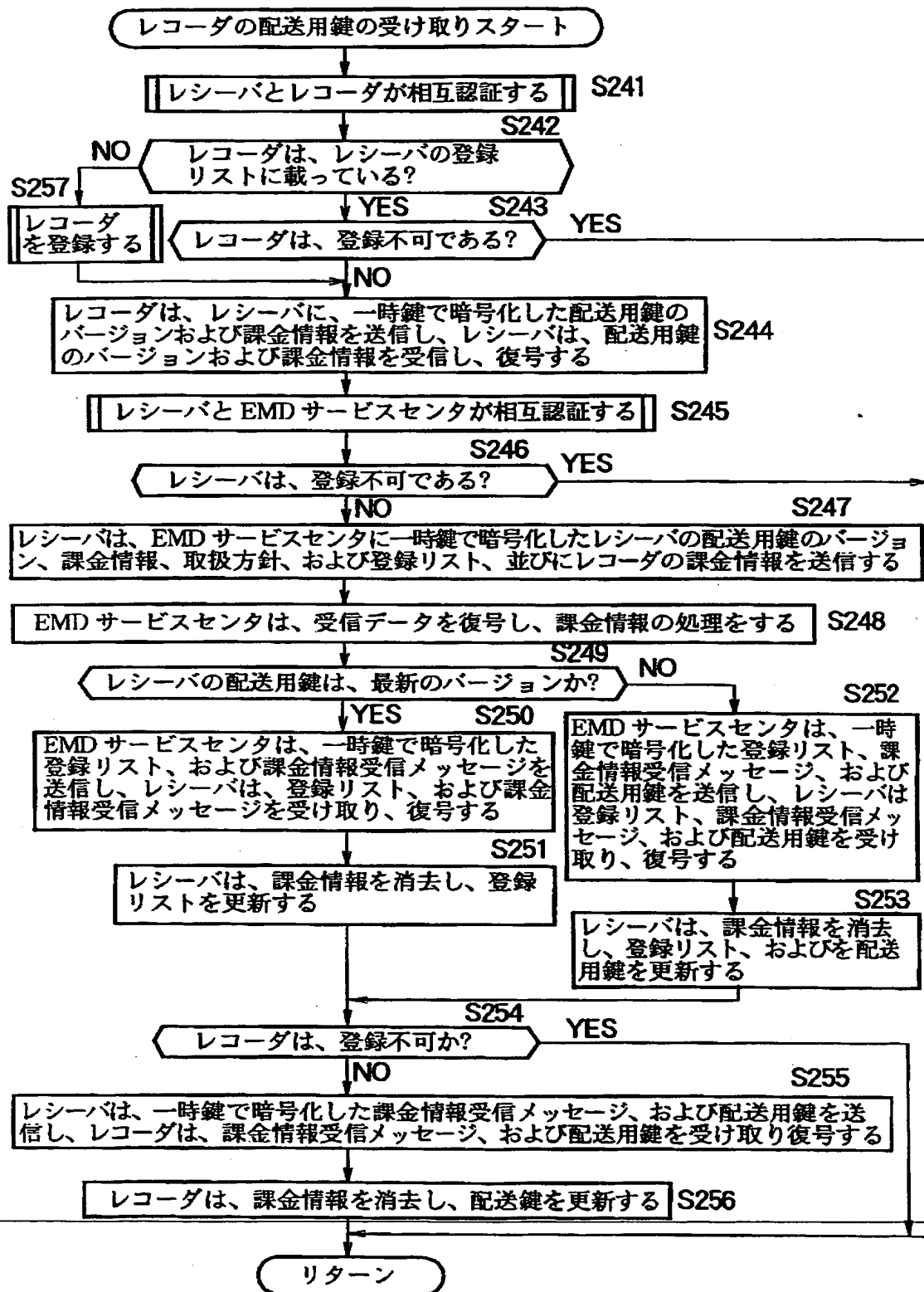
【図 44】



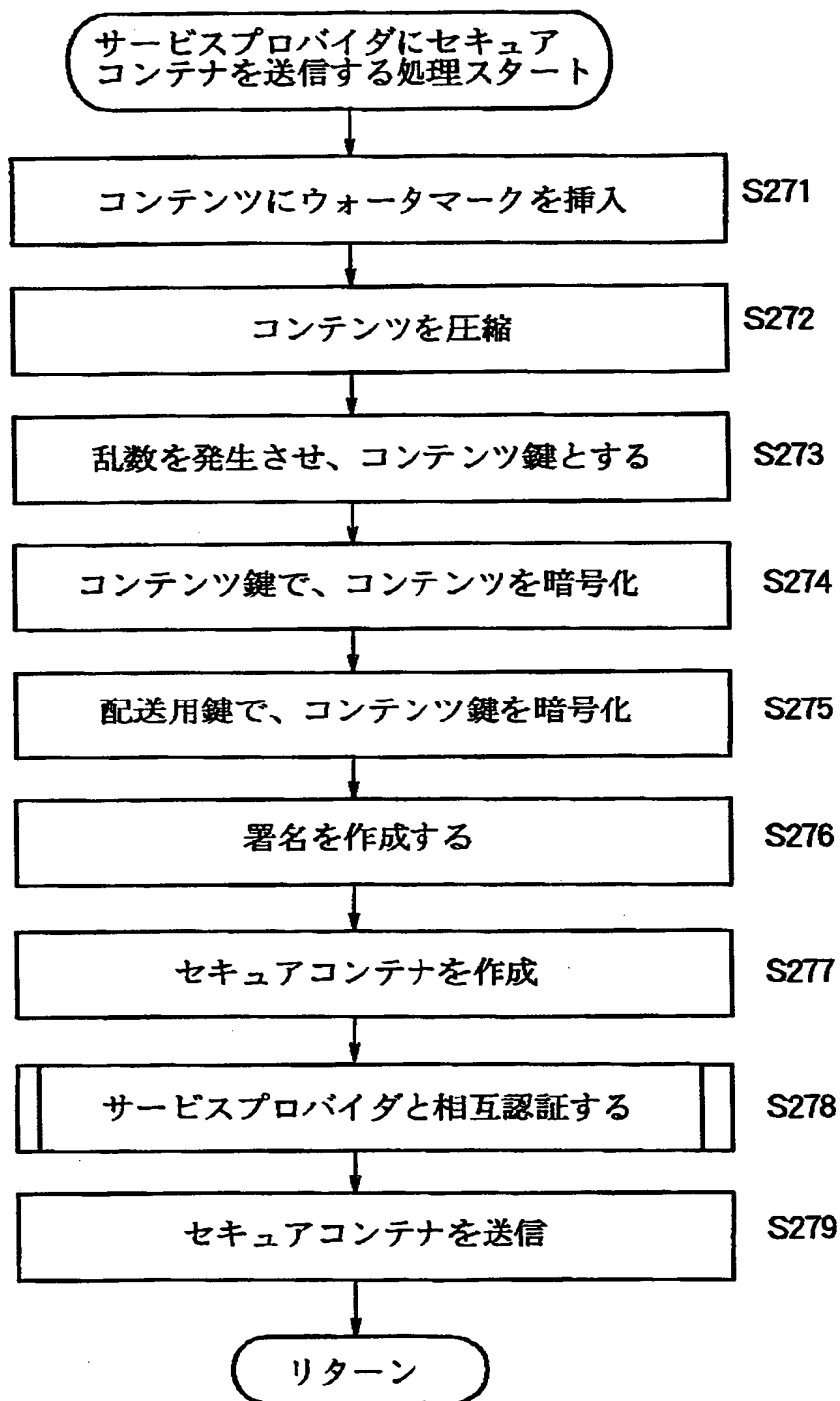
【図 4 5】



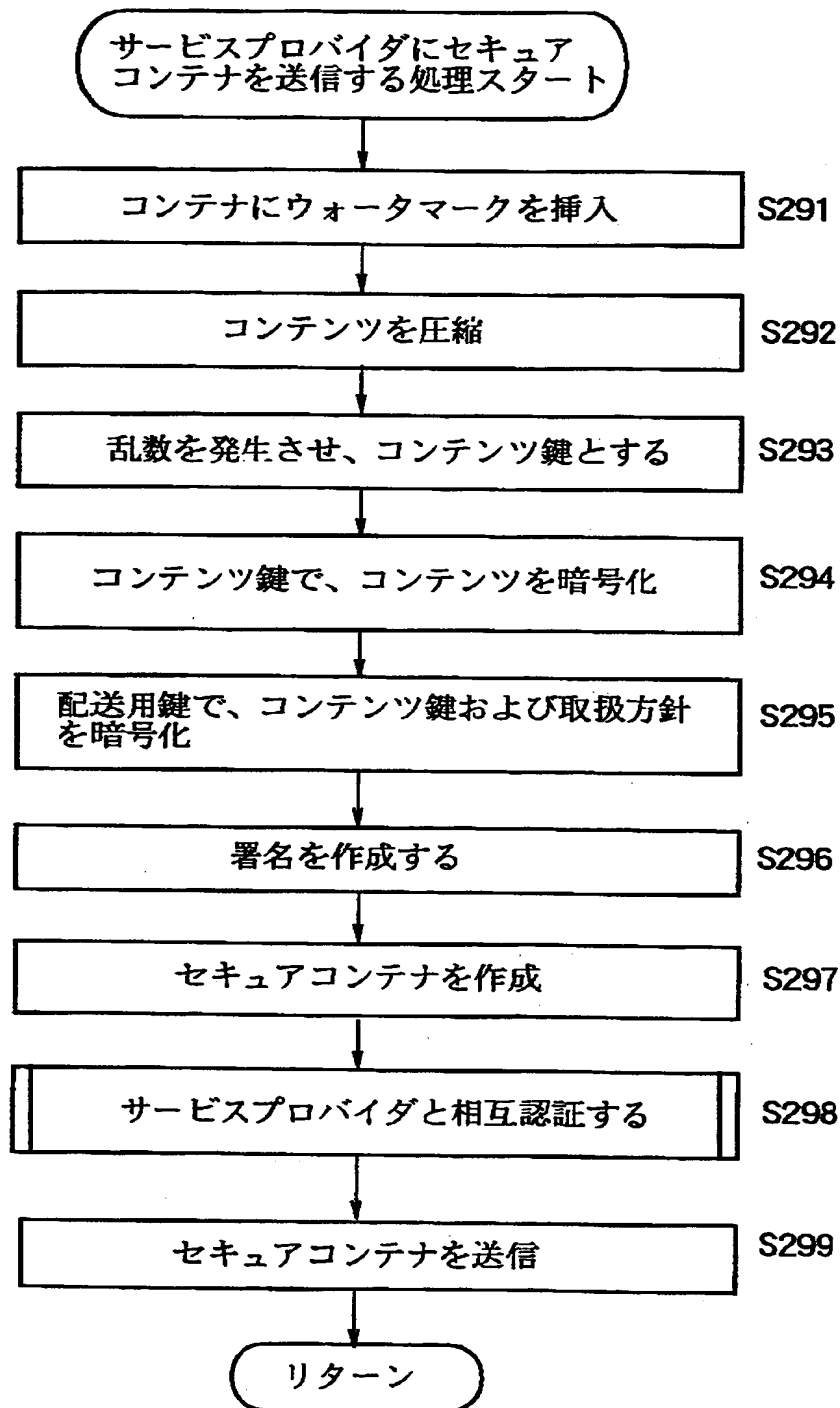
【図 4 6】



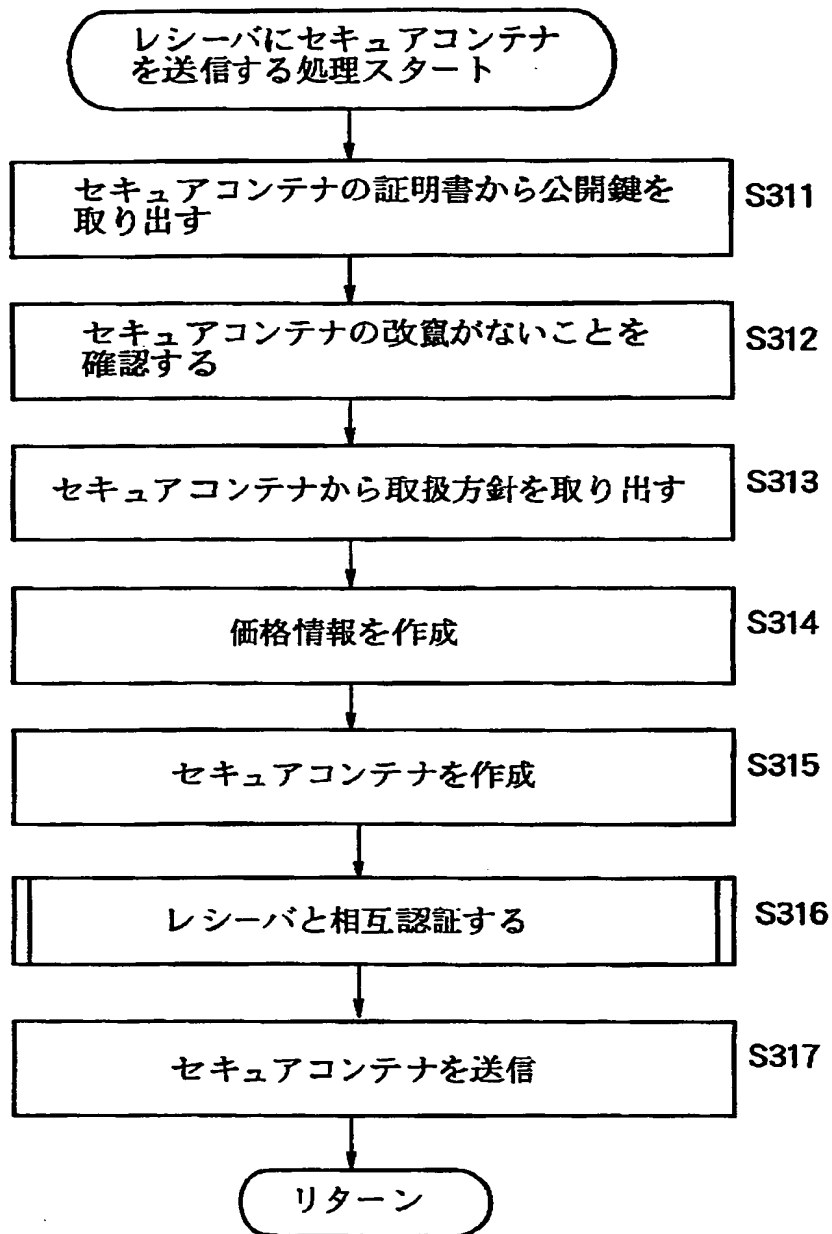
【図47】



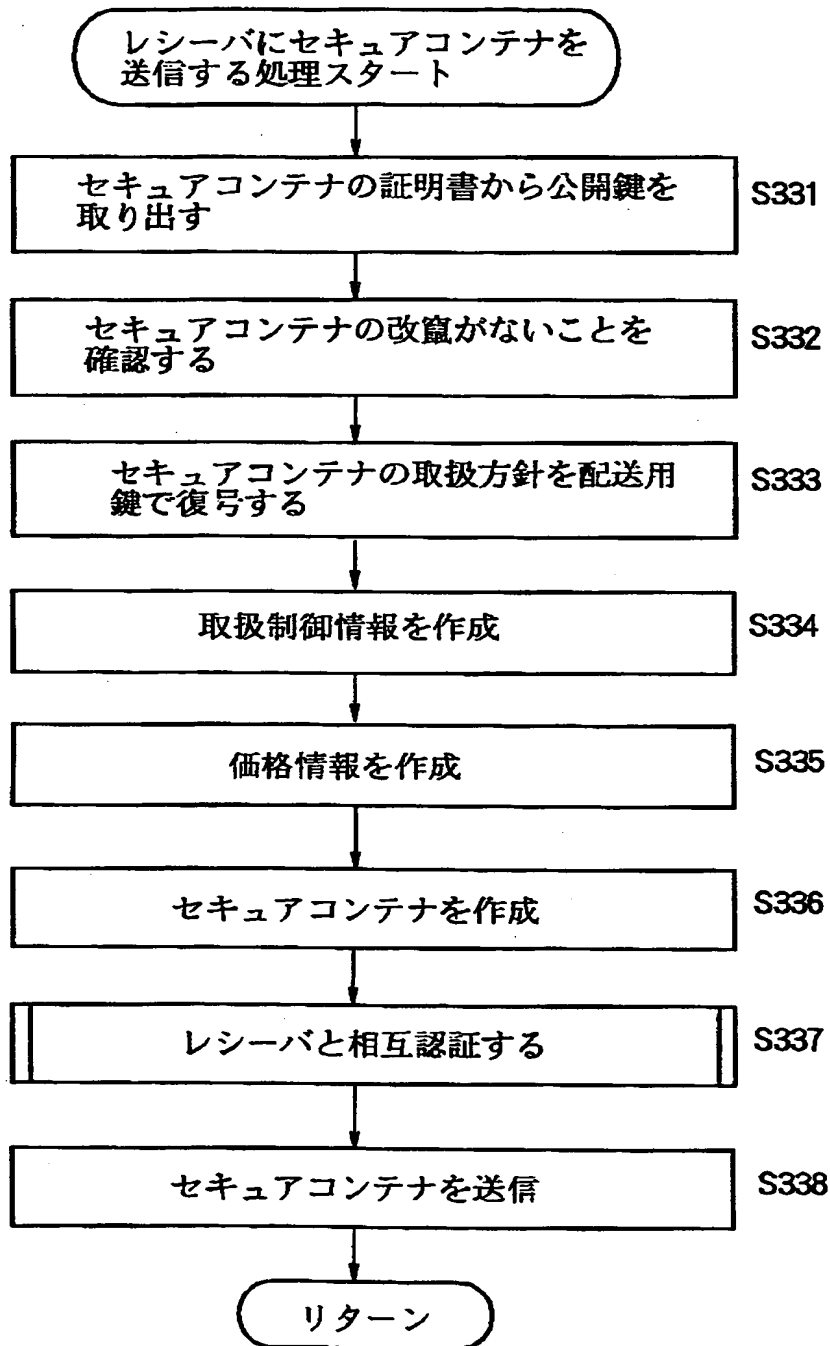
【図 48】



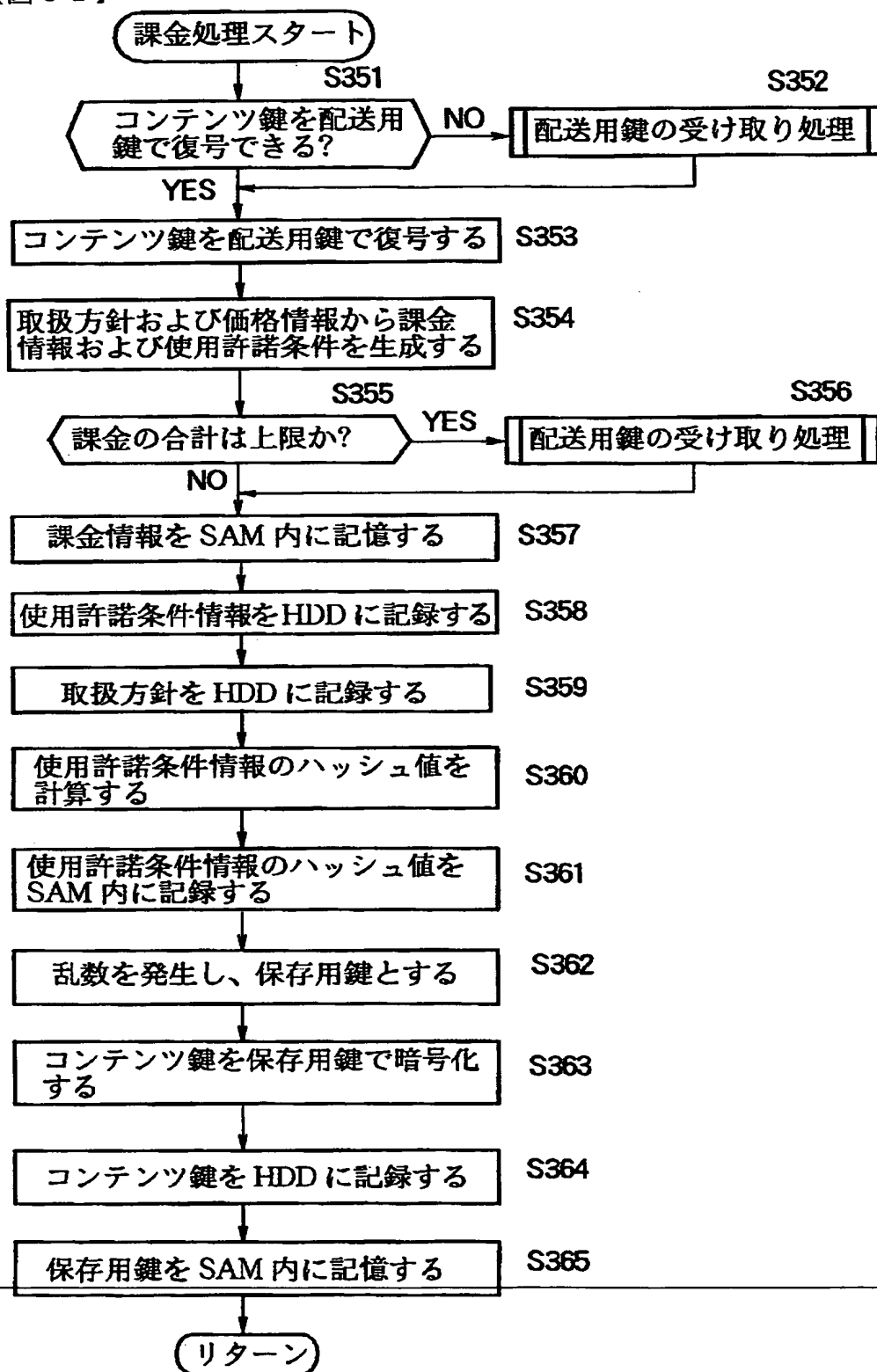
【図49】



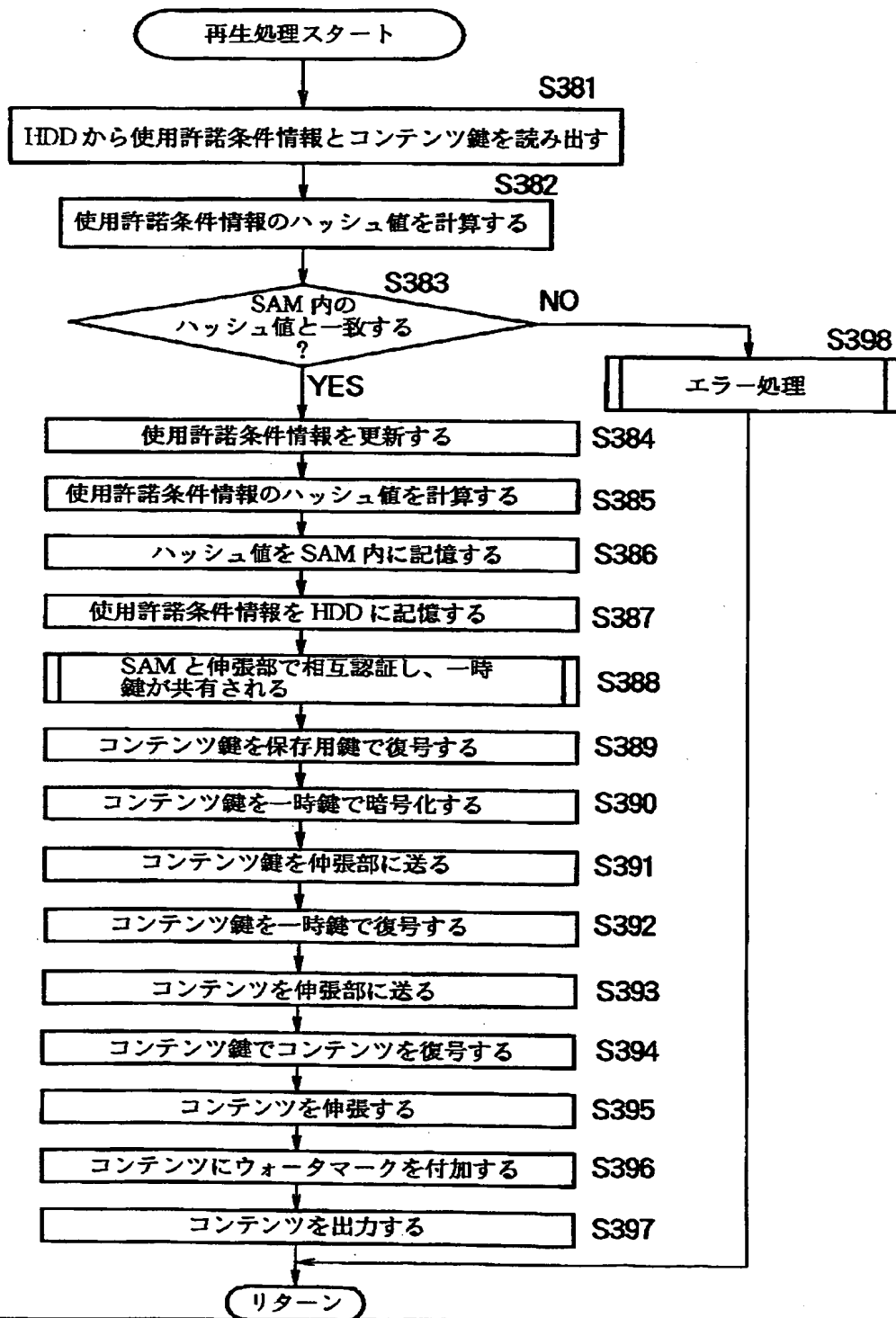
【図 50】



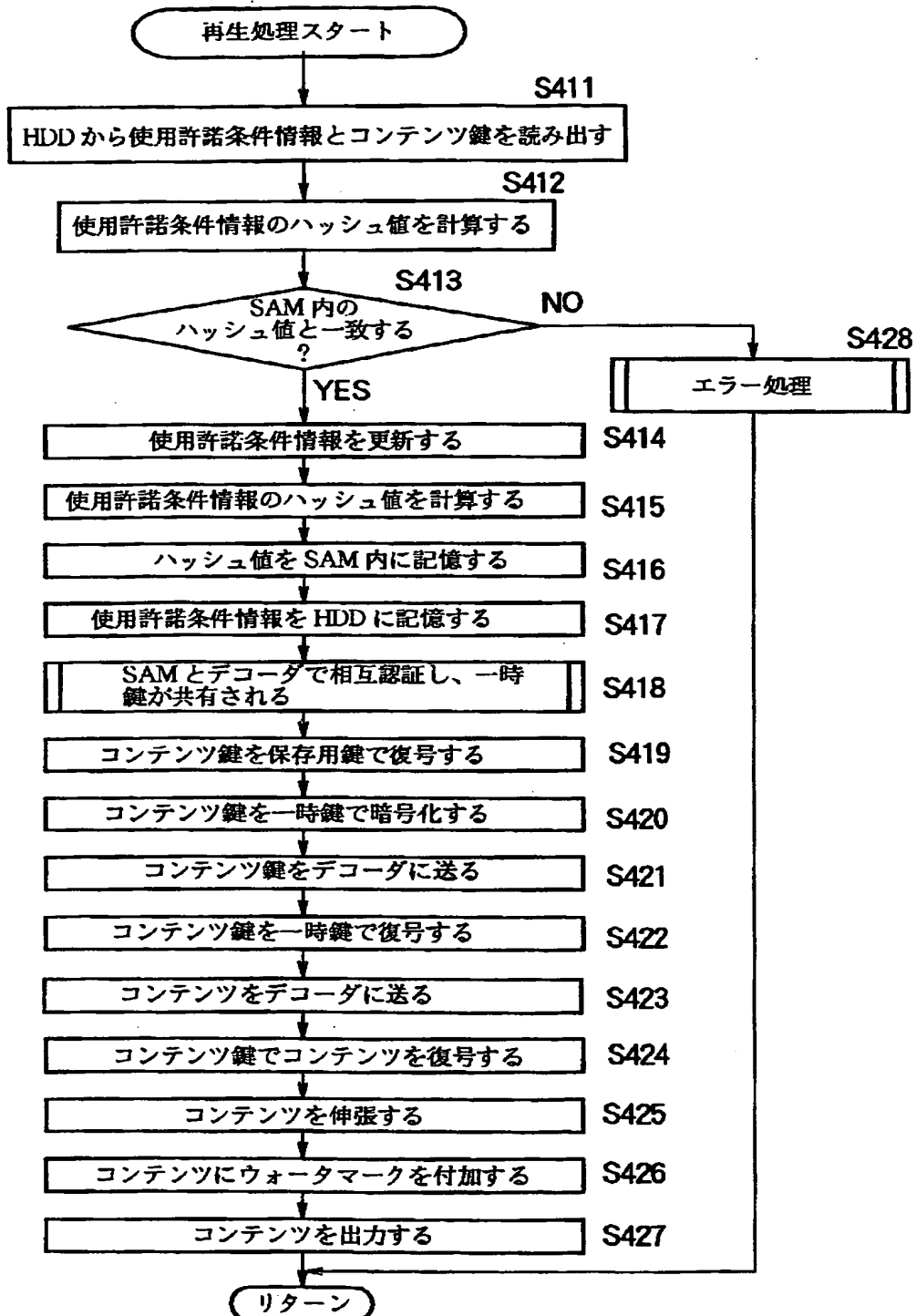
【図 51】



【図 5 2】



【図 53】



【書類名】 要約書

【要約】

【課題】 不正に対する安全性を保持したまま、必要な情報を外部に記憶できるようにする。

【解決手段】 相互認証モジュール 71 は、装着された外部記憶媒体と相互認証し、暗号化ユニット 93 は、所定の鍵で所定の情報を暗号化する。

【選択図】 図 10

【書類名】 職権訂正データ
【訂正書類】 特許願

<認定情報・付加情報>

【特許出願人】
【識別番号】 000002185
【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号
【氏名又は名称】 ソニー株式会社
【代理人】 申請人
【識別番号】 100082131
【住所又は居所】 東京都新宿区西新宿 7 丁目 5 番 8 号 GOWA 西新
宿ビル 6 F 稲本国際特許事務所
【氏名又は名称】 稲本 義雄

出 願 人 履 歴 情 報

識別番号

[000002185]

1. 変更年月日	1990年 8月30日
[変更理由]	新規登録
住 所	東京都品川区北品川6丁目7番35号
氏 名	ソニー株式会社